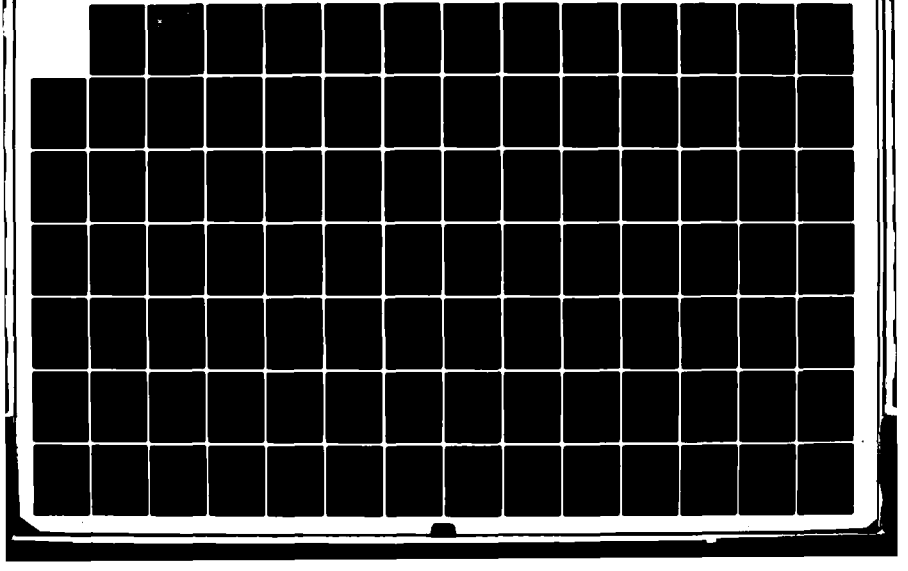
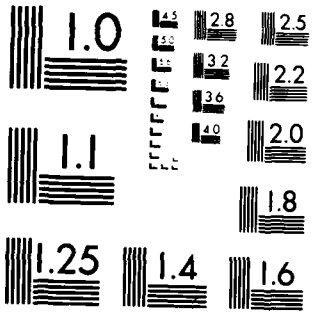
AD-A134 583 SYSTEM INTEGRATION AND INTERFACE TRANSITION ISSUES(U) 1/3
DEFENSE COMMUNICATIONS ENGINEERING CENTER RESTON VA
APR 77 DCEC-TR-2-77

UNCLASSIFIED F/G 17/2 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

TR 2-77

DEFENSE COMMUNICATIONS ENGINEERING CENTER

AD-A134583

TECHNICAL REPORT NO. 2-77

SYSTEM INTEGRATION AND INTERFACE TRANSITION ISSUES

APRIL 1977

DTIC
ELECTE
NOV 8 1983
D

DTIC FILE COPY

Approved for public release; distribution unlimited

83 11 08 166

UNCLASSIFIED Mar 1977
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER TR 2-77	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) SYSTEM INTEGRATION AND INTERFACE TRANSITION ISSUES		5. TYPE OF REPORT & PERIOD COVERED Technical Report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s)		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Defense Communications Engineering Center Systems Engineering Division, R700 1860 Wiehle Ave., Reston, Va. 22090		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS N/A
11. CONTROLLING OFFICE NAME AND ADDRESS Same as 9		12. REPORT DATE March 1977 13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) N/A		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A

16. DISTRIBUTION STATEMENT (of this Report)

(Unlimited)

App... Distri...

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

(Unlimited)

18. SUPPLEMENTARY NOTES

Review relevance 5 years from submission date.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

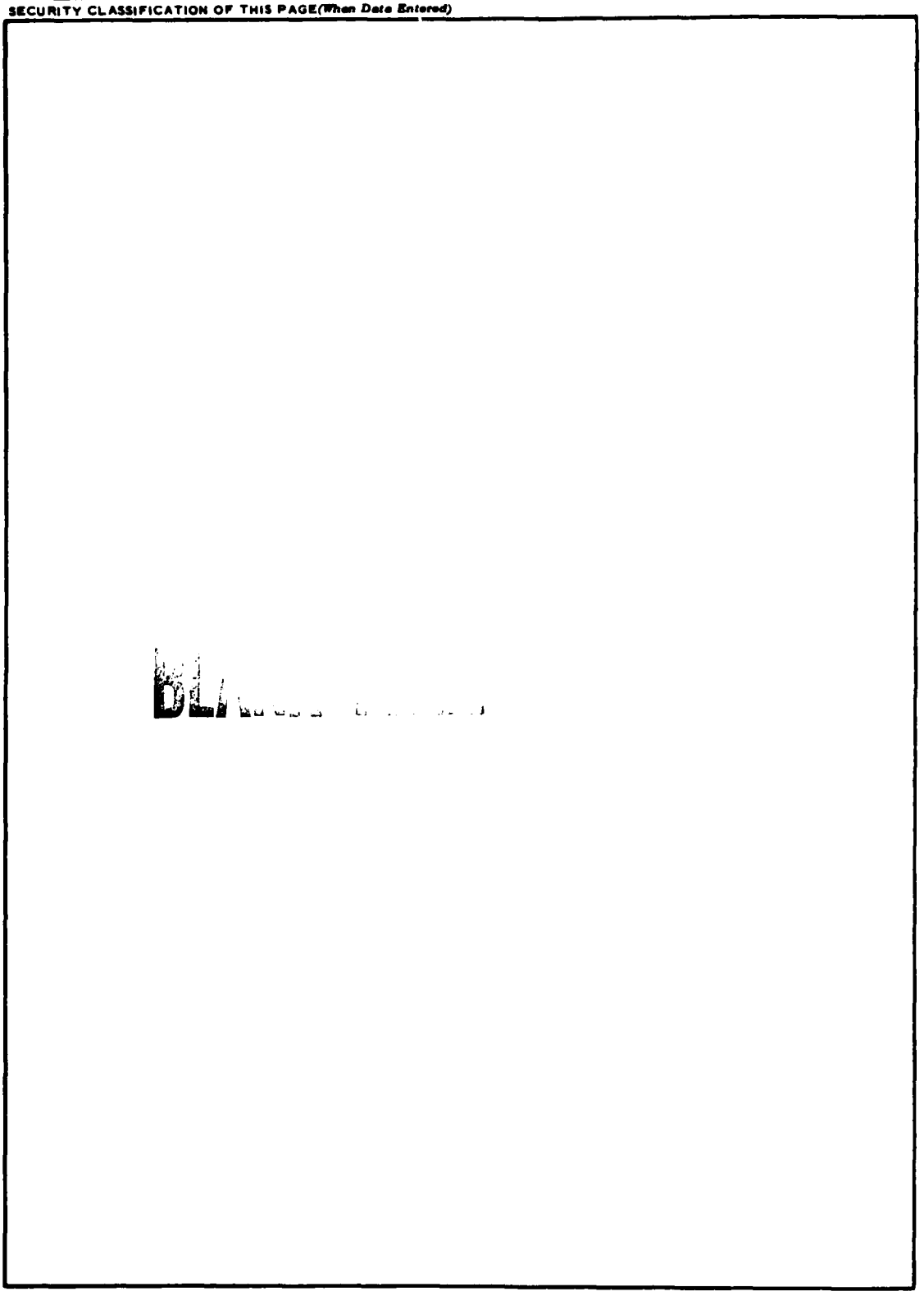
System Interfaces	Program Objectives
System-Level Issues	Digitization Strategy
DCS Transition	Dynamic Stability

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This Technical Report documents systems engineering and analysis in support of the DCS Plan FY 80/90. Transition issues regarding system integration and interfaces among subsystems are treated. Six system-level issues perceived as the most critical are defined and analyzed. The most critical and the most promising areas for continuing studies are recommended.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)



Accession For
NTIS GPA&I
DTIC TAB
Unannounced
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A/1

TECHNICAL REPORT NO. 2-77

SYSTEM INTEGRATION AND INTERFACE TRANSITION ISSUES

MARCH 1977

Prepared by:

- Systems Design Branch

DTIC COPY INSPECTED

Technical Content Approved:

W. L. CHADWELL
Chief, Systems Engineering Division

Approved for Release:

R. H. LEVINE
Deputy Director

FOREWORD

The Defense Communications Engineering Center Technical Reports (TR's) are published to inform interested members of the defense community regarding technical activities of the Center, completed and in progress. They are intended to stimulate thinking, encourage information exchange, and provide guidance for related planning and research. They are not an integral part of the DoD PPBS cycle and should not be interpreted as a source of program guidance.

Comments or technical inquiries concerning this document are welcome, and should be directed to:

Director
Defense Communications Engineering Center
1860 Wiehle Avenue
Reston, Virginia 22090

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

LIST OF FIGURES

LIST OF FIGURES (Cont'd)

LIST OF FIGURES (Cont'd)

LIST OF TABLES

LIST OF TABLES (Cont'd)

LIST OF TABLES (Cont'd)

I. INTRODUCTION

1. PURPOSE

This technical report documents systems engineering and analysis in support of the Defense Communications System (DCS) Plan FY 80/90. Its principal purposes are: to identify and analyze technically oriented issues and problems of interest to Defense Communications Agency (DCA) engineers, to assess the system impact of alternative solutions to the interface and integration issues, to assess cost and performance impacts, to identify specific areas for further in-house addressal or contractor support, and to identify specific areas for MILDEP support.

This document is expected to provide management with technical analyses necessary to select subsystem directions in areas of emphasis that will evolve from the current DCS configuration to an architecture capable of satisfying future DCS requirements.

2. RELATIONSHIP TO DCS PLANNING DOCUMENTATION

This document and two other related technical reports provide technical support for the DCS Plan FY 80/90. The others are TR 1-77, "Planning and Programming Transition Issues", and TR 3-77, "Operational and Maintenance Manning Reduction Studies". TR 1-77 addresses those management-oriented system design issues and the architectural alternatives available for determining major program directions and relative emphasis. TR 3-77 addresses both near-term and long-term methods of reducing military manning requirements for DCS facilities, particularly in the overseas regions. Together, these three reports provide the technical investigations and analyses to support the DCS Plan FY 80/90.

The DCS Plan provides the significant system design issues, objectives, alternatives, and selected course of action for further development and ultimate implementation. Specific implementation actions and detailed project developments necessary to field and support a worldwide telecommunications system are contained in the DCS Five-Year plans (FYP), Subsystem/Project Plans (S/PP), major program management plans, and similar documents. An interaction between the DCS Plan and the existing programming and implementation documents, including those being developed, is required in order to effect any major modifications to current programs.

3. SCOPE

The scope of the document is defined by the specific system issues designated to receive continuing system design and engineering attention. They are discussed in the following paragraphs.

For the subsystems and elements which characterize the DCS, certain information about the health and disposition of the system is required. This information must originate with and be exchanged by the various subsystems and elements. The questions that must be addressed for these actions are specifically what information is required, for what purpose is it needed (importance and timeliness), to whom must it be transmitted, and how will the transmittal be accomplished? All of these questions are particularly important relative to the efficient maintenance, operation, management and control of the DCS. An assessment of all of these questions, except the last, has been made and detailed examples are presented.

DCS plans specifically address both transmission and switching subsystems. Certain incompatibilities in the detailed specifications of the transmission and switching equipment cause a system interface problem. Three conceptual solutions are proposed and various alternatives are analyzed to determine the strengths and weaknesses of each.

The transition of the DCS towards an all-digital communications system raises the question of how this digitization is to be accomplished. The current 64 kb/s PCM strategy is bandwidth inefficient compared to a lower rate delta modulation (DM) alternative. Channel capacity and spectrum allocation problems may force the use of a lower rate DM strategy. Such a strategy is analyzed and compared to the current PCM approach.

The DCS secure voice population is composed of isolated subscribers, small bodies of subscribers, and large communities of subscribers. These classes give rise to certain alternatives for interfacing them with the DCS backbone network. Alternatives to perform this action, ranging from individual secure terminals, bulk encryption, and PBX-to-PBX security are developed and tradeoffs are performed.

Major costs for any system that requires both hardware and software packages are incurred in the definition, design, development, and testing of the software. The significance of this system issue is addressed and potential areas for greatest savings are discussed. Approaches to software design are developed and the programming language issue is detailed. An approach for the reduction of software costs is given.

The DCS, as a system, is characterized by periodic transients resulting from actions taken to overcome equipment failures. These transients can cause instability within the system. This instability can be viewed, for example, in terms of fault propagation in that an equipment failure may cause other equipments to fail, or may result in unnecessary maintenance activity to parts of the system that are functioning within normal tolerances. This issue is addressed in the context of the effect of timing and synchronization and signal encryption on system stability, and the fault modes that can occur which influence system stability.

These major issues are addressed as if they were self-contained. However, as can be inferred from the issue discussions, they are indeed connected and some of the discussions pervade several of the issues. This is intended. It is also intended that the addressal of the issue alternatives will provide a clearer picture of the system architecture and the options available to management.

4. ASSUMPTIONS, CONSTRAINTS, AND APPROACH

In the development of this report, current DCS plans and programs were considered. These were the foundation and constraints from which issues were defined and developed, and from which alternative solutions were advanced. The structure of the architecture for existing DCS programs, for a given issue area, provided the basis from which to begin. All assumptions and constraints for each issue are stated.

The approach taken in this report is to show what capabilities exist, those that can be achieved, and what benefits can be gained.

II. SUBSYSTEM INTERFACES

1. INFORMATION EXCHANGE AMONG MAJOR DCS SUBSYSTEMS AND ELEMENTS

Circa 1980-1982, the Defense Communications System will be a hybrid consisting of subsystems which are both analog and digital in nature. The newer digital elements will be introduced via major DCS programs such as:

- Digital European Backbone, Phase I through IV
- Pacific Digitization
- Defense Satellite Communications System
- AUTOSEVOCOM Phase II
- AUTODIN Phase II
- System Control

The implementation of these programs will have a significant impact on the information needs of the major DCS subsystems and their organizational elements. The information needs must be first identified and tabulated. This process is the prime concern of this section. Subsequent to identification/tabulation a specification control process must be initiated to ensure that the DCS subsystem and elements interact as conceptualized. Finally the information flow must be translated into specific hardware/software design if the well-being of the DCS is to be sustained.

a. Elements and Subsystems. The major DCS subsystems are transmission and switching. Interacting with these subsystems are the DCA mission element, the maintenance/operations element, and the user element. These are depicted in Figure 2-1.

The prime mission of the Defense Communications Agency (DCA) is to exercise operational direction and management control over the DCS. Actual operation and maintenance of the subsystems are the responsibility of the MILDEP's. The user and access areas have been historically considered non-DCS elements. These major subsystems and elements must interoperate properly if system operation and performance objectives are to be realized.

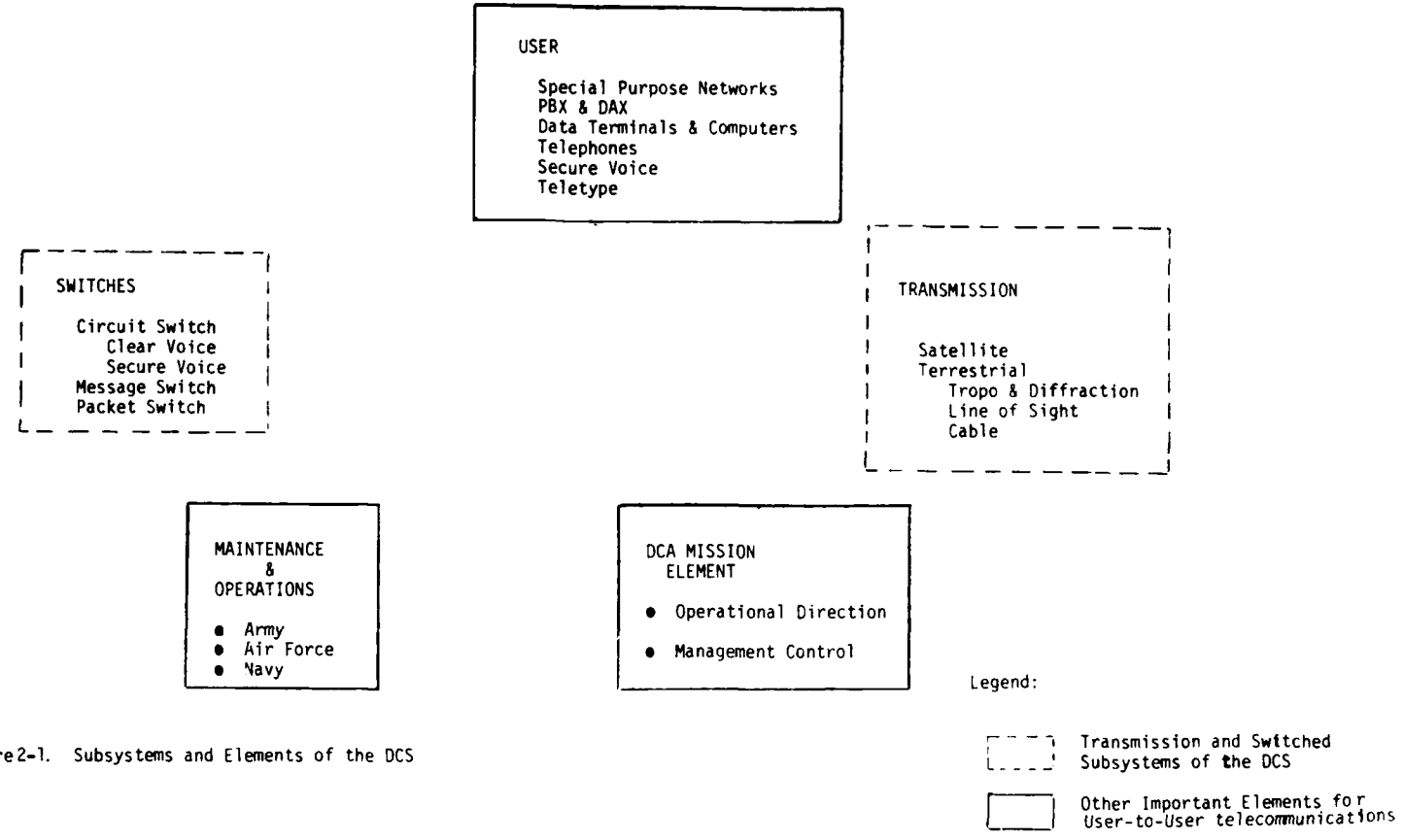


Figure 2-1. Subsystems and Elements of the DCS

Ideally, data characterizing the operation and performance of a communications system should be conveyed to those elements most suited to react and respond to the information received, and most capable of initiating corrective action. The information needs to be considered serve the maintenance, operational direction, and management control elements responsible for the day-to-day operation, maintenance, short-term direction, and long-term management functions of the DCS. The user element, beneficiary of the mentioned functions, also interacts with DCS networks by receiving network status information and providing or requesting self status.

(1) Maintenance. The function of the maintenance element is to restore degraded system service to a normal operation level. Depending on the availability and skill of the on-site maintenance level, status information, consisting of failure and degradation alarm indicators, is used to initiate appropriate maintenance responses. The frequency and timeliness of the status information depend on whether an immediate or delayed response by the maintenance element is required.

Local maintenance action generally involves routine testing, fault isolation activities, and minor module repair or replacement, and is usually confined to personnel associated with the technical control facility (TCF), patch and test facility (PTF), switch transmission media and user equipments. Complex maintenance actions such as repair or replacement of major hardware/software components involve servicing skills usually beyond the capability of the local personnel. Recent developments in communications system design have emphasized increased system availability and reduced dependence on costly and numerous on-site maintenance personnel by providing built-in diagnostic testing, redundancy and restoral features which can be activated locally or remotely. These features include automatic hardware alarm and software fault check; module level testing, troubleshooting and replacement; and module/equipment level redundancy switching and bypass functions. For the most part, however, these features have not been designed into the DSCS segment of the DCS.

(2) Operational Direction. The primary responsibility of the operational direction element is to ensure timely system responsiveness to the requirements of the DCS subscribers. Its mission includes the implementation of contingency plans and the optimization of the availability of communications resources for the use of approved critical users. Operational direction involves not only network reconfiguration and service extension, but also service restoral and denial. This is carried out by exercising direction over various subordinate operational elements, by alerting appropriate operational elements, or possibly by exercising direct control over system elements. The operational direction

element utilizes information related to nodal and link status, nodal configuration and data base, network traffic status, and network performance. Nodal capacity, configuration, and data base information provides the input for exercising responsive control and direction over network operations. Network traffic, status, and performance information assists the operational direction element in detecting and isolating system-level traffic congestions.

(3) Management Control. This element is characterized by long-term functions required to manage and improve the system. It includes the establishment of standards, practices, and procedures for prescribing system performance, operation, and maintenance. It requires non-real-time system information and consists mainly of data pertaining to system performance and system availability This information when correlated with the network configuration data base may be utilized for planning and controlling system modification and improvement.

(4) User. The user element is generally concerned with terminal equipments and access lines and network interface status information. Billing and community of interest performance data are also of interest to the user. Only status information indicating service degradation is provided to the user element on a real time basis.

b. Information Exchange Characterization. Information exchanges among subsystems and elements can be functionally characterized by need, importance, and timeliness of the information. Each piece of information has associated with it some measure of each of these characteristics. For example, an information transfer from one element or subsystem to another is either needed or not needed, important or relatively unimportant, and real time or not real time. While these are admittedly binary classifications, there are varying degrees for each characteristic.

(1) Need and Importance. The need for and importance of information are direct measures of its usefulness at the receiving end. For example, timely link and node status information is needed by the maintenance element in detailed form and by the operational direction element in summarized format. It is not needed on a real time basis by either management control or user elements. It is, however, information essential to the missions of maintenance and operational direction, and therein derives its importance.

(2) Timeliness. A key characteristic of information exchange is the speed of relay and speed of response (i.e., information interaction time). Table 2-I summarizes the system information required by the four elements and the time parameters associated with transmission to and response from the elements.

TABLE 2-I. INFORMATION REQUIREMENT OF MAINTENANCE, OPERATIONAL DIRECTION, MANAGEMENT CONTROL, AND USER ELEMENTS

Information element	Equipment Status & Alarms		Nodal/Link Status & Major Alarms		Nodal Configuration and Nodal Data base		Nodal Traffic Status		System Performance and general Status	
	FR	DR	FR	DR	FR	DR	FR	DR	FR	DR
Maintenance/ Operation	X	X	X		X	X				
Operational Direction			X		X		X		X	
Management Control		X		X		X		X		X
User	X	X							X	X

FR - fast relay and/or response.

DR - delayed relay and/or response.

The timeliness of information exchange and control interaction is related to the sampling of monitored parameters and frequency of relaying them to the appropriate control elements. It also relates to the time required for the application of controls to effect improved communications services, particularly to critical users. The above parameters vary depending on the causes of service degradation, and except for limited applications [1] are not yet defined.

(a) Maintenance And User Element. The maintenance element receives real-time equipment status and alarm data in sufficient detail to enable fault-isolation to equipment or module level. The user element is provided with general status information from the network to prevent unnecessary fault-isolation or maintenance activities.

(b) Operational Direction Element. With the evolution and development of the various planned DCS subsystems, particularly system control, the operational direction element is envisioned to be capable of near real-time interaction, utilizing the following information flow categories:

- Nodal/link status and major alarms
- Nodal data base, including nodal configuration
- Nodal traffic status and performance (data from which system degradation can be extracted; e.g., network grade of service and speed of service).

In general, the nodal data base component (changes in nodal configuration, tables, etc.) of the total information exchange will probably be significant during crisis situations. The processing and storage of this information could be shared or integrated with similar management control functions. System performance data may find use in assessing the short term system health, as opposed to the management control function which evaluates the long term system health.

Presently, the operational direction element exercises very limited real-time control. In the future, enhanced capability will depend almost entirely on the SYSCON subsystem implementation. It must incorporate features that gather, process, store, display, summarize, and evaluate or provide trends from raw or preprocessed data. It will also provide for appropriate control action either by directing local subordinate elements or by initiating the control action directly.

The control actions directed and applied by the operational direction element are in response to system-level problems, such as major links outages or global switch traffic congestion. These control actions will complement and utilize switch, TCF, and transmission subsystem control capabilities.

(c) Management Control Element. The interaction of this element with DCS subsystems is performed entirely on a non-real-time basis, principally because this element does not exercise functions that have an immediate impact on the network subsystem.

(3) Interaction Time. The information categories and associated information interaction time for each of the elements are given in Table 2-II. A general description and examples of the information flows are also provided.

c. Information Exchanges Tables. The subsystem and elements that are involved in the information interchange may be broken out as follows:

- Transmission - consisting of satellite and terrestrial media (government-owned and leased)
- Switches - involving circuit, message and packet switched networks (government-owned and leased)
- DCA Mission Related Elements - consisting of management control and operational direction
- Maintenance and Operation
- User.

The element and subsystem interconnection is represented in Figure 2-2. Note that some functional blocks are not paired with other blocks since it is anticipated that certain elements will not require information exchange. Table 2-III is a matrix identifier for the information tables that follow. Each number in the matrix designates the table in which the indicated element/subsystem pair information exchange may be found.

Thirteen element/subsystem information flow pairs are presented in Tables 2-IV through 2-XVI. Each pair, whether element-to-element, element-to-subsystem, or subsystem-to-subsystem, depicts the category of information, specific examples relevant to the category, and the utility of the information. The tabulation is not intended to be complete or exhaustive, but it does demonstrate the type of information interchange that should be considered for both near-term implementation and long-term objectives.

TABLE 2-II. INFORMATION CATEGORIES AND ASSOCIATED INFORMATION INTERACTION TIME

Element	Information Category	Information Transfer & Control Response State	General Description & Examples
Maintenance/ Operation	Equipment status and alarm	FR/FR	Major equipment failures (initiating major alarms) resulting in immediate communications outages or degradations. *Examples:* Failure of critical nodal subsystems (nodal power, environmental control, etc). Failure of critical communications components having no redundancy, backup or bypass (baseband input to the LOS transmitter) Failure of redundant, backup or bypass component subsequent to failure of main component (MUXs, diversity receivers, switch memory, etc).
		FR/DR	Equipment failure (initiating minor alarms) resulting in limited or no communications outages or traffic congestion. Examples: Failure of components having redundant backup on bypass elements (MUX, diversity receivers, JST trunks)
	Nodal Configuration & data base	DR/DR	Modifications in non-local nodal components and configurations. Installation of new facilities and equipments.
Operational Control	Nodal/Link status & alarms	FR/FR	Major alarms affecting communications of critical users or large number of common users and requiring relatively prolonged maintenance restoral activity. Examples: Reports-switch outages, Hazcons, nodal (radio, MUX, etc) outages. Controls-circuit and group reconfigurations, switch bypass, destination code cancellation.
		FR/DR	Major alarms affecting communications of critical users or large number of common users resulting in relatively short outage time (estimated). Prolonged outages, communications degradations, traffic congestions, affecting small number of common users.

LEGEND
- FR - Fast Relay
- FR/FR - Fast Relay, Fast Response
- FR/DR - Fast Relay, Delayed Response
- DR - Delayed Relay

TABLE 2-II (Cont'd). INFORMATION CATEGORIES AND ASSOCIATED INFORMATION INTERACTION TIME

Element	Information Category	Information Transfer & Control Response State	General Description & Examples
Operational Control (Continued)		DR	Summaries of terminal, access line, and network status affecting user service.
	Traffic status	DR	Billing data
	System Performance	DR	Network and community of interest performance measures (availability, point-to-point GOS).
			Examples: Reports-access line and/or user terminal failures. *Controls-prompt O&M elements to carry out* maintenance action.
	Nodal Configuration & data base	FR	Changes and modifications of nodal data base. Modifications to thresholds.
			Examples: Switch and nodal circuit reconfigurations. Implementation of circuit restoral. Implementation of software module loading (changes in software-routing, classmarks, etc).
	Traffic status	FR/FR	Indications of potential global traffic congestions.
			Examples: Reports - Local switch initiated controls. Trunk and groups occupancies. Call offered/blocked/preempted by precedence. Control-trunk redirectionalization, load control threshold modifications, routing modifications.
	System Performance	FR/FR	Network reconfiguration in response to short term trending indication (long-term objective).
			Examples: Rise in traffic congestion. Rise in BER on digital groups.

TABLE 2-II (Cont'd). INFORMATION CATEGORIES AND ASSOCIATED INFORMATION INTERACTION TIME

Element	Information Category	Information Transfer & Control Response State	General Description & Examples
Management Control	Nodal/Link status and alarms Nodal Configurations and data base Traffic status System Performance	DR	Information applicable to long-term system availability and system performance. Data base management, billing data, community of interest data. Examples: Same as for operational direction element except all information is summarized on non-real time basis. Point-to-point traffic patterns. Long-term traffic pattern shifts.
User	Equipment Status & alarms	FR	Prolonged network outages and degradations having direct impact on user-to-user service. Access line and user terminal outages and degradations detected at network (periodic or upon request loop back testing).

FR - fast relay

FR/FR - fast relay, fast response

FR/DR - fast relay, delayed response

DR - delayed relay

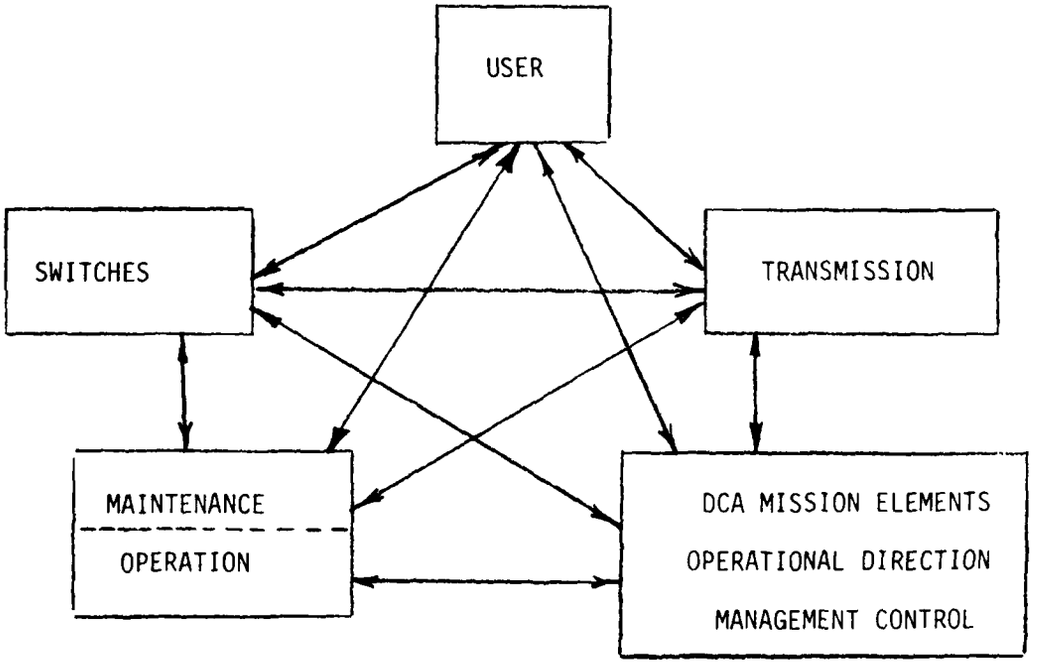


Figure 2-2. Information Exchange Paths Among The DCS Subsystems and Elements

NOTE: See Figure 2-1 for detailed descriptions of the subsystems/elements

TABLE 2-III MATRIX IDENTIFYING TABLES SUMMARIZING INFORMATION

FLOW BETWEEN SUBSYSTEMS AND ELEMENTS PAIRS

From \ To	Tx	Sw	User	Operational Direction	Management Control	Maintenance/ Operation
Transmission Subsystem		IX	XI	XIII	XII	XV
Switch Subsystem	VIII		XI	VI	IV/V	XVI
User Element	XI	XI			X	
DCA Operational Direction Element	XIV	VII				
DCA Management Control Element	XII	V	X			
Maintenance/ Operation Element	XV	XVI				

TABLE 2-IV. INFORMATION FLOW FROM NETWORK SWITCHES TO MANAGEMENT CONTROL ELEMENT

INFORMATION FLOW FROM NETWORK SWITCHES TO MANAGEMENT CONTROL ELEMENT (Non-real time - NRT)	EXAMPLES	UTILITY
1. Traffic statistics and network performance data summaries.	1. Summaries extracted from the following: Circuit Switch Calls offered/blocked/preempted by trunk, trunk group and precedence. Number of trunks busy. Total calls blocked by common equipment (by precedence). Calls per busy period (by type or precedence) including: Total volumes Loop to loop traffic Node pairs traffic Calls exceeding specified thresholds (dial tone delay). Message Switch Messages on queue in-transit, overflow, or intercept storage. Oldest message in storage. Amount of storage occupied. Packet Switch Input, relay and output buffer utilization by priority. Average number of simultaneous connections for host computer. Number of retransmissions on link and end-to-end basis. Looping condition.	1. Computation of network performance measures: Grade of Service Call Completion Rate Speed of Service End-to-end throughput Determination of switch storage and buffers utilization. Determination of access line and trunk and common equipment utilization. Indication of long-term traffic patterns. Indication of long-term traffic congestion patterns. Indication of potential routing problems. Recognition and monitoring of community of interest traffic. Processing of billing data. Long-term evaluation of trunk and access line quality (e.g., AUTOVON transmission related trouble cards, retransmission reports). Evaluation of system thresholds.

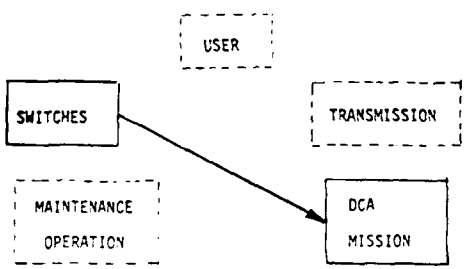


TABLE 2-IV (Cont'd). INFORMATION FLOW FROM NETWORK SWITCHES TO MANAGEMENT CONTROL ELEMENT

INFORMATION FLOW FROM NETWORK SWITCHES TO MANAGEMENT CONTROL ELEMENT (NRT)	EXAMPLES	UTILITY
	1. Summaries extracted from the following: M.S. and P.S. Traffic Volumes - incoming and outgoing (message) blocks, packets, segments or other traffic units on backbone and access lines - totals by categories. Rejects and discards of messages, packets, segments. (with reason given) Blocking statistics by category of traffic. Trace and header extracts. Distribution of traffic by messages, blocks, segments, characters, etc. Number of calls preempted - by precedence. Total calls attempted.	
2. Switch equipments, switch transmission, access lines and terminals, status summaries	2. Summaries extracted from the following: Switch outages. Switch Hazcons. Status of critical switch hardware and software functions. [1]Switch IST and access line status. [1]Terminal equipment outages. Transmission related trouble cards (O/S AUTOVON switch)	2. Evaluation of system availability and module reliability summaries. Determination of prolonged switches or subscriber outages and coordination with appropriate. O&M agencies when required. Correlation with traffic status data.
3. Data Base status	3. Changes in: Directory tables Trunk grouping Routing tables Media related parameters (transmission delays) Thresholds Registers, buffer and storage allocations	3. Management control of switch configuration and data bases. Update of switch software modules. Evaluation of modifications.

[1]Assumes switch process and/or switch associated PTF scans performances status of transmission lines and activates loop-back testing procedures to isolate line equipment and user interface faults (access lines, multiplexers, crypto-equipment, subscriber interface and terminals.)

TABLE 2-IV (Cont'd). INFORMATION FLOW FROM NETWORK SWITCHES TO MANAGEMENT CONTROL ELEMENT

INFORMATION FLOW FROM NETWORK SWITCHES TO MANAGEMENT CONTROL ELEMENT (Non-real time - NRT)	EXAMPLES	UTILITY
4. Summaries of switch and system control (operational direction) initiated controls.	4. Throttling (M.S., P.S.) Line and trunk load control (C.S.) Routing updates Destination code cancellation Resetting of thresholds and allocations Switch and transmission reconfiguration.	4. Assessment of effectiveness control actions. Correlation with traffic status data.

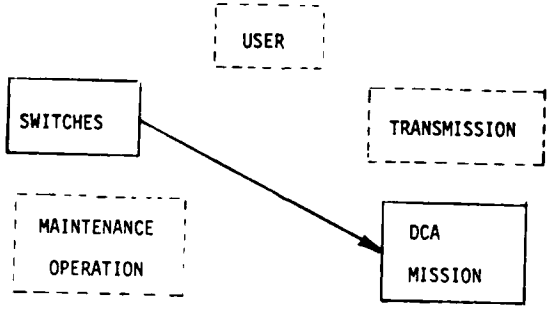


TABLE 2-6 Information Flow From Network Switches To Management Control Element

TABLE 2-V. INFORMATION FLOW BETWEEN MANAGEMENT CONTROL AND NETWORK SWITCHES

INFORMATION FLOW BETWEEN MANAGEMENT CONTROL AND NETWORK SWITCHES (NRT)	EXAMPLES	UTILITY
1. Improvement (as a result of long term evaluation) of switch associated routines and tables.	1. Modification (improvement) of Routing algorithm Transmission configurations Switch Software modules.	1. Implement improvement programs resulting from long-term evaluations.
2. Monitoring and thresholds selection.	2. Lines, trunks and trunk groups to be monitored. Selection of thresholds setups (by precedence or category) such as: Trunk restriction Line load control Buffer and storage allocation	2. Facilitate selective data collection for subsequent evaluation.
3. Request and adjustment of reports.	3. Change in frequency, sampling intervals details of reports.	3. Minimize or expand data used for management control function.

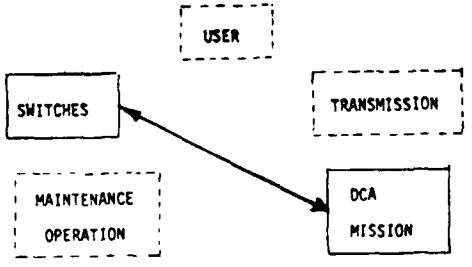


TABLE 2-VI. INFORMATION FLOW FROM NETWORK SWITCHES TO OPERATIONAL DIRECTION ELEMENT

INFORMATION FLOW FROM NETWORK SWITCHES TO OPERATIONAL DIRECTION ELEMENT (NRT)	EXAMPLES	UTILITY
1. Traffic status and network performance parameters (short-term summaries or processed data)	By priority, precedence or traffic category: Trunk, trunk group, access line utilization. Number of IST busy (C.S.) Utilization of common equipment, status of senders and receiver registers or calls queues (C.S.) Input, relay and output buffer utilization (P.S.) Queues on in-transit, overflow or intercept storage (M.S.) Scheduled heavy traffic loads of outgoing or incoming traffic (M.S., P.S.)	1. Detection and anticipation of local and global traffic congestions. Criteria for initiating global control actions.
2. Switch status	2. Switch outages, Hazcons (hardware and software; - power, environmental and timing subsystem) Switch degradation (in terms of handling rated capacity)	2. Facilitate control and operational decisions to minimize total network impact.
Switch associated IST, access line and terminal status	[1]IST, Critical user access lines outages or degradation. BER of digital channels (e.g., CCIS) Terminal outages of critical users.	Anticipation and isolation of global system problems. Interaction with appropriate O&M agencies.
	[1]Transmission related trouble cards (O/S VON)	
Switch/transmission timing and Synchronism	[1]Loss of channels group synchronism Timing buffer overflow	
	[1]Loss of timing	

[1]This information is normally conveyed to the transmission subsystem. However, when possible and practical this information may be used to isolate 'global' system problems (e.g., network timing, or network reconfiguration.

TABLE 2-VI (Cont'd). INFORMATION FLOW FROM NETWORK SWITCHES TO OPERATIONAL DIRECTION ELEMENT

INFORMATION FLOW FROM NETWORK SWITCHES TO OPERATIONAL DIRECTION ELEMENT (NRT)	EXAMPLES	UTILITY
3. Switch configuration and data base status	3. Changes in (acknowledgment of implementing) Trunk grouping Mix of Media Routing tables Threshold settings.	3. Facilitate reconfiguration decisions with respect to affected node and total network.
4. Initiation and Acknowledgment of control actions (on occurrence)	4. Line load control (C.S.) or throttling (P.S., M.S.) Trunk restriction (C.S.) Class mark restriction Destination code cancellation Routing modifications Time-out control (P.S., M.S.) Minimize Queue, storage or pooled devices realiocation Link and trunk directionalization Fault-isolation and restoral Programs reload/restart Traces routine activation (M.S., P.S.) Threshold modifications.	4. Depict control state being applied at each node.

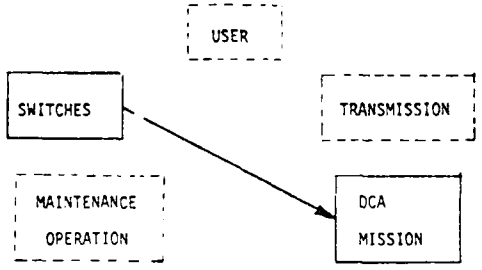
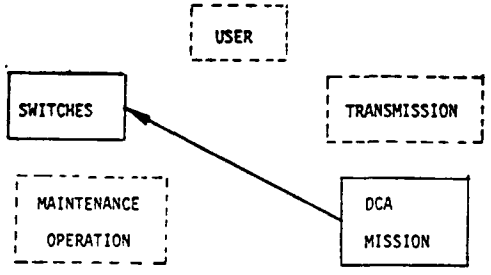


TABLE 2-VII. INFORMATION FLOW FROM OPERATIONAL DIRECTION ELEMENT TO NETWORK SWITCHES

INFORMATION FLOW FROM OPERATIONAL DIRECTION ELEMENT TO NETWORK SWITCHES	EXAMPLES	UTILITY
1. Network reconfigurations (near-real time)	1. Directives: Modify IST and acces lines configurations. Bypass of switch terminations. Reallocation of trunks and trunk groups. Directionalization of trunks and links.	1. Reaction to contingencies. (outages, degradation and drastic changes in traffic patterns.) Restoral actions.
2. Traffic control (near-real time)	2. Initiation and termination of: [1] Trunk restriction [1] Line load control Destination code cancellation Routing changes Threshold resetting Buffers and storage allocations Software module changes.	2. Alleviation of network traffic congestions. Control response to outages.



[1] These controls are normally applied locally.

TABLE 2-VIII. INFORMATION FLOW FROM SWITCH SUBSYSTEM TO TRANSMISSION SUBSYSTEM

INFORMATION FLOW FROM SWITCH SUBSYSTEM TO TRANSMISSION SUBSYSTEM*	EXAMPLES	UTILITY FAULT ISOLATION
1. IST and access lines status	1. Status changes Out-of-service Degraded Normal Examples: trunk group pilot below threshold (O/S VON)	1. Initiate maintenance/restoral activities by operational and maintenance elements of transmission subsystem.
2. Switch status changes	2. [illegible]-service [illegible] - Hazcon condition [illegible]	2. Prepare operational elements for critical subscribers restorals. Prevents unnecessary user initiated trouble-shooting activities.
3. Demand assignment configuration (satellite)	3. Routing, [illegible]	3. Effective satellite resource utilization.

*Exchange can take place via operational control element.

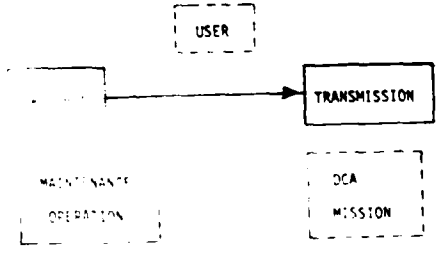
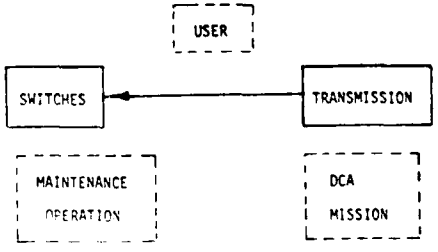


TABLE 2-IX. INFORMATION FLOW FROM TRANSMISSION SUBSYSTEM TO SWITCH SUBSYSTEMS

INFORMATION FLOW FROM TRANSMISSION SUBSYSTEMS TO SWITCH SUBSYSTEMS*	EXAMPLES	UTILITY
1. IST and access line status change	1. Status: Out-of-service Degraded Pre-empted by critical user Under test or maintenance condition (anticipated time duration) Normal	1. Prevent routing attempts over faulty transmission. Facilitate appropriate responses: Alternate routing Routing changes Altroute procedure Busy out calls to failed destination.
2. IST Reconfiguration	2. Identification of transmission route characteristics. links groups circuits	2. Compensate for new transmission characteristics, e.g., time delay over satellite links. Update routing tables. Update transmission oriented classmarks, e.g., availability of bulk encryption on new link.
3. Links status change	3. Transmission channel groups status. Out-of-service. Degraded.	3. Same as 1 above.



*Exchange can take place via operational control element.

TABLE 2-X. INFORMATION EXCHANGE BETWEEN USER ELEMENT AND MANAGEMENT CONTROL

INFORMATION EXCHANGE BETWEEN USER ELEMENT AND MANAGEMENT CONTROL (NRT)	EXAMPLES	UTILITY
A. From User to Management Control		
1. Change in traffic patterns	1. Community of Interest. Mix of traffic categories: Voice - Secure Clear Data - Message I/A, Q/R Bulk Facsimile Narrative/record	1. Long-term improvement and extension plans. Examples: Add or directionalize links Update routing tables.
2. Change in Operating Procedure	2. Operating Hours (peak traffic load) of tributary	2. Same as above.
B. *From Management Control to User*		
1. Traffic statistics, network and access area performance and utilization.	1. Summaries of network performance criteria, i.e., GOS, CCR, SOS. Distribution or originating traffic and utilization of access lines. Community of interest traffic data. Billing data.	1. Feedback to customer on network performance. Billing information.

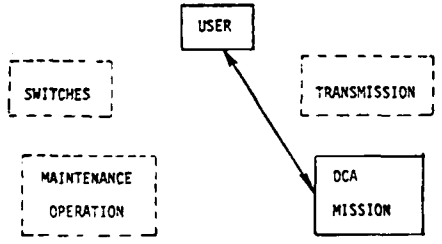


TABLE 2-XI. INFORMATION EXCHANGE BETWEEN USER ELEMENT AND NETWORK (TRANSMISSION AND SWITCHES SUBSYSTEMS)

INFORMATION EXCHANGE BETWEEN USER ELEMENT AND NETWORK (TRANSMISSION AND SWITCH SUBSYSTEMS)	EXAMPLES	UTILITY
A. From Network to User Subsystem		
1. Backbone, access lines, switches and user's equipment interface status.[2]	1. Condition: Out-of-service Degraded Normal	1. Prevent needless users maintenance actions. Allows special purpose networks to make intelligent network control decisions. Initiates maintenance actions at the local plant.
2. Out-of-service test notices[2] (must have subscriber approval)	2. Time of initiation, restoral and estimated duration of test.	2. Provide user with option to preempt or continue with the out-of-service test.
3. Subscriber traffic restriction and interruption.	3. Appropriate signaling.	3. Prevent needless user attempts to obtain service or take maintenance action.
B. From User Subsystem to Network		
1. Equipment (terminal - data, voice, DAX, PBX, MUX) status.	1. Condition: Out-of-service Degraded Normal	1. Divert traffic to secondary address of a dual-homed subscriber. Initiate altroute procedure. Minimize attempts to communicate with affected destination.
2. Request for loop-back test.[2]	2. Status of local plant transmission and equipment interface.	2. Facilitate fault-isolation activities.

[2]Assumes TCF or switch associated PTF scans performance status of homed transmission lines and activates loop-back testing procedures to isolate line equipments and user interface faults (IST, access lines, multiplexers, crypto-equipment, subscriber interface, and terminals).

TABLE 2-XII. INFORMATION EXCHANGE BETWEEN TRANSMISSION AND MANAGEMENT CONTROL ELEMENTS

INFORMATION FLOW BETWEEN TRANSMISSION SUBSYSTEM AND MANAGEMENT CONTROL CENTER ELEMENT	EXAMPLES	UTILITY
A. From Transmission Subsystem to Management Control		
1. Status of links and node.	1. Summaries of: Outage reports - specified by: Transmission links Equipment type Location Outage time Degraded performance reports - specified by: Transmission links Probable causes Location Time duration	1. Data related to transmission resources reliability and availability providing and input for transmission improvement plans. Interaction with appropriate O&M agencies.
2. Data base and transmission configuration status.	2. Changes in: Nodal records Circuit layout records Transmission capacity	2. Update transmission data bases.
3. Quality Assurance and Fault Isolation Data (long-term summaries).	3. Link and group quality extracted from the following transmission related parameters: Absolute or relative BER Format violations Frame synchronism pattern error rate Eye pattern Decoder errors Synchronism at multiplexers and bulk-encryption devices Timing buffers overflow	3. *Isolation of system pervasive faults. Long-term trending analysis with ultimate goal of performance prediction and appropriate network control actions.

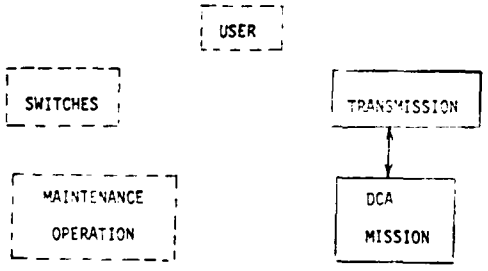


TABLE 2-XII (Cont'd). INFORMATION EXCHANGE BETWEEN TRANSMISSION SUBSYSTEM AND MANAGEMENT CONTROL ELEMENTS

	Frequency offsets RSL G/T, C/T (satellite) Base band loading (applied to FDM radio and FDMA satellite) Slot noise measurement (analog)
Channel quality extracted from the following:	Lack of modem activity BER or digital distortions Format violations.
Eye pattern Timing offsets Analog channel parameters such as:	*Idle channel noise* Signal power Phase distortion Impulse noise etc., (similar to ATEC measurements)

*The value of trending parameters of digital transmission is probably of limited value.

TABLE 2-XIII. INFORMATION FLOW FROM TRANSMISSION SUBSYSTEM TO OPERATIONAL DIRECTION ELEMENT

INFORMATION FLOW FROM TRANSMISSION SUBSYSTEM TO OPERATIONAL DIRECTION ELEMENT	EXAMPLES	UTILITY
1. Nodal/Link records. (On occurrence when status changes or near-real time).	1. Changes in records including: Circuit, groups - patched, added, reconfigured. Circuits, groups - in/out-of-service (duration) Communication spare capacity	1. Update nodal data base.
2. Nodal/link status	2. Outage reports - specified by: Transmission links Equipment type Location Estimated outage time Degraded performance reports - specified by: Transmission links Probable causes Location Time duration (estimated) Effort on link capacity	2. Facilitate control decisions related to critical user restoral and Network reconfiguration.
3. Operational status	3. Monitoring of (satellite) allocated - Frequencies Power Rate (bandwidth) Time slots Orbit and pointing control Jamming/non-jamming condition	3. Insure adherence to allocated bounds with appropriate directives and control actions if these are not met. Initiation of anti-jamming actions and configurations.
4. Acknowledgment of directives	4. Operational directives	4. Insure directive implementation.

TABLE 2-XIV. INFORMATION FLOW FROM OPERATIONAL DIRECTION TO TRANSMISSION SUBSYSTEMS

INFORMATION FLOW FROM OPERATIONAL DIRECTION TO TRANSMISSION SUBSYSTEM	EXAMPLES	UTILITY
1. Operational directives and commands.	1. Restorals, extension and reconfiguration of links and circuits. Use of transmission spare capacity. Change in specified allocations. Bandwidths Frequencies Power Number of subscribers Channel slots	1. Increase communications availability to critical users.

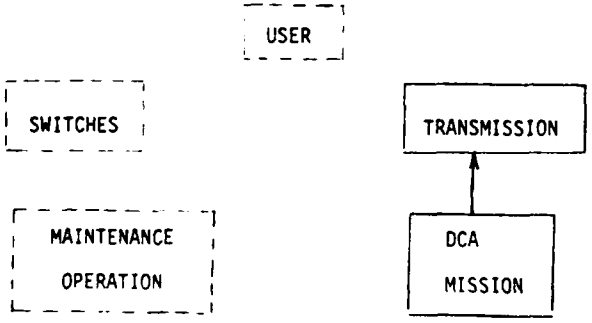


TABLE 2-XV. INFORMATION EXCHANGE BETWEEN TRANSMISSION SUBSYSTEM AND MAINTENANCE ELEMENT

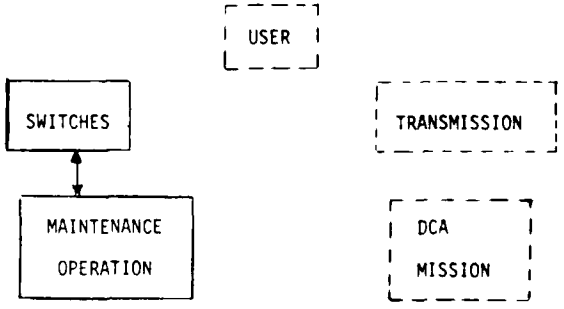
INFORMATION EXCHANGE BETWEEN TRANSMISSION SUBSYSTEM AND MAINTENANCE ELEMENT*	EXAMPLES	UTILITY
A. From Transmission to Maintenance (RT)		
1. Transmission status and major alarms.	1. Alarms associated with: Transmitter/Receiver - RSL Baseboard loading Slot noise Frequency offsets BER Multiplexers - Frame synchronism Timing buffers overflow Input and output ports signal transitions Encryption devices - Synchronism Signal transitions Timing subsystem - Timing offsets Timing sources operation Power subsystem - Power supplies Facility subsystem - Air conditioning	1. Indication of faults or initiation of fault-isolation procedures (such as loop-back testing) when necessary. Initiation of maintenance actions.
B. From Maintenance Element* to Transmission Subsystem		
1. Restoral status.	1. Equipment restored or out-of-service. Time estimation for restoral.	1. Status indication.

*Assumes Maintenance Element is remoted from the site.

TABLE 2-XVI. INFORMATION EXCHANGE BETWEEN NETWORK SWITCHES AND MAINTENANCE ELEMENT

INFORMATION EXCHANGE BETWEEN NETWORK SWITCHES AND MAINTENANCE ELEMENT*	EXAMPLES	UTILITY
A. From Switches to Maintenance (RT)		
1. Alarms and status information.	1. Alarms associated with: Switch modules (hardware, software), common equipment, transmission interface, timing, power and facilities subsystems outages and degradations.	1. Indication of faults or initiation of fault-isolation procedures (such as loop-back testing) when necessary. Initiation of maintenance actions.
B. From Maintenance Element to Transmission		
1. Restoral status.	1. Equipment restored or out-of-service. Time estimation for restoral.	1. Status indication.

*Assumes Maintenance Element is remoted from site.



III. AUTOSEVOCOM/DIGITAL TRANSMISSION INTERFACE

1. SWITCH/TRANSMISSION SUBSYSTEM INCOMPATIBILITY

Circa 1980-1982 the Defense Communications Systems will be of a hybrid nature. The overseas backbone transmission plant will be extensively digitized both in Europe and the Pacific and will serve to route both analog and digital traffic. The transmission technical control facilities (TCF), the interface point between the traffic originating elements and the backbone transmission subsystem, will require enhanced capabilities mainly in interfacing with traffic originating from digital sources. In addition, the prospect of accommodating AUTOSEVOCOM II switch requirements in Europe by utilizing the TRI-TAC developed AN/TCC-39 has further highlighted the need for an interface between the Digital Radio and Multiplex Acquisition (DRAMA) transmission subsystem and the switch subsystem. A viable interface solution is necessary since the switch configurations for digital transmission groups are not adequate for DCS application. The basic incompatibility between the two subsystems, (i.e., the breakdown and recombination of inter-switch trunks) requires an investigative look at alternative solutions.

a. Generic Technical Control Subsystem. Figure 3-1 generically represents a TCF partitioned into analog and digital sections. The analog portion provides the same functions as present day analog TCF's including circuit conditioning, signaling and ancillary equipment for testing dedicated and switched voice, facsimile, teletype, and medium-speed modem driven data circuits. The digital portion of the TCF provides signal conditioning, buffering, grouping and multiplexing functions for synchronous data streams. Combining and interfacing asynchronous data streams also occurs. The facility will provide the normal technical control functions of circuit restoral and extension, testing and fault isolation, coordination with operation/maintenance elements, and reporting to operational direction and management control elements.

b. Circuit Distribution at TCF. The partitioning of the TCF into analog and digital parts is based on functional requirements. These parts will not accommodate similar circuit loading requirements. Based on projected circuit and traffic requirements (1985-88), it appears that the bulk of the circuit appearances at the TCF will be analog. Secure voice circuits will comprise less than 10%, and data circuits about 24% of the total circuits. Figure 3-2 illustrates a typical link cross-section with these percentages identified.

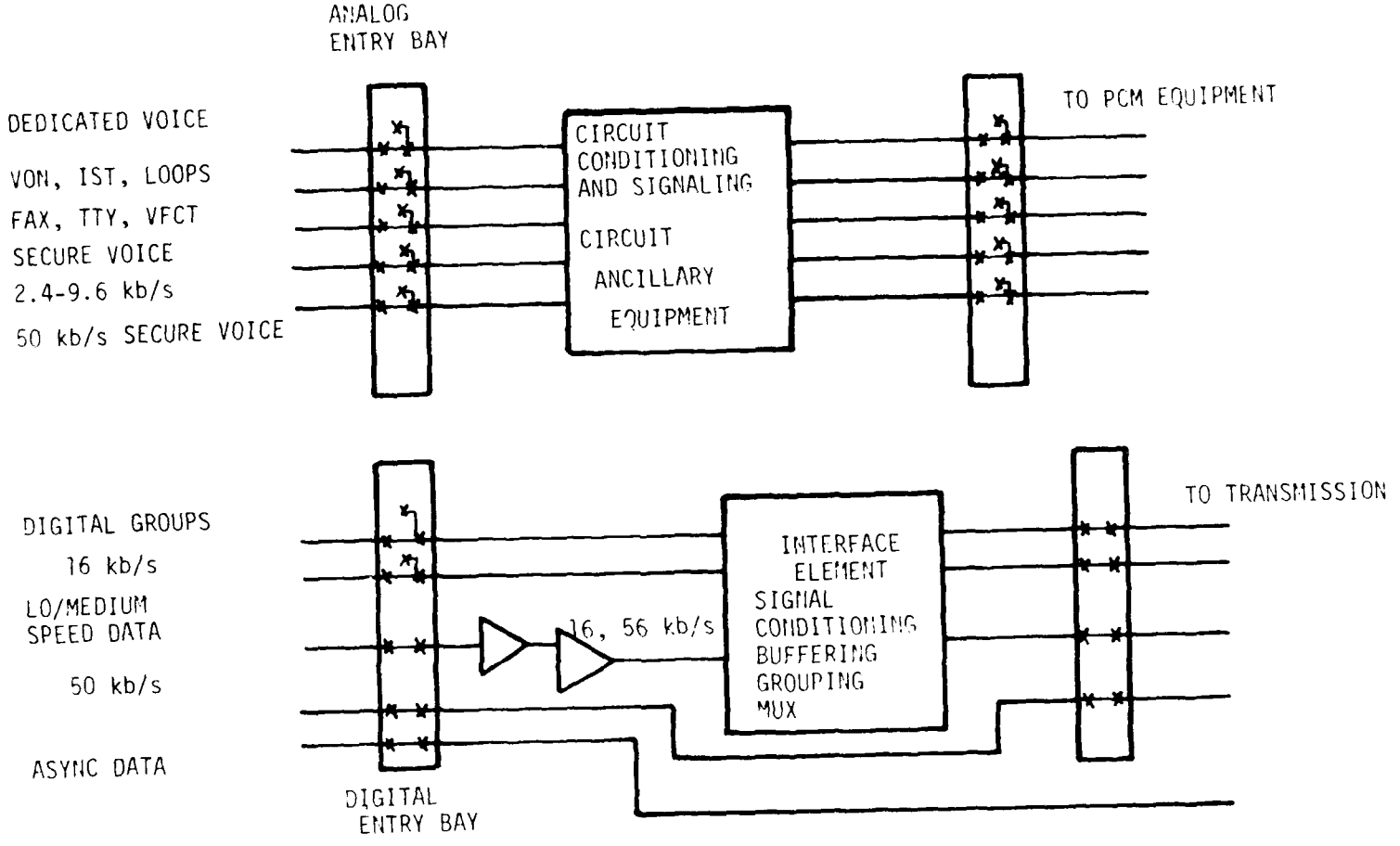


Figure 3-1. Generic Representation of Technical Control Facility

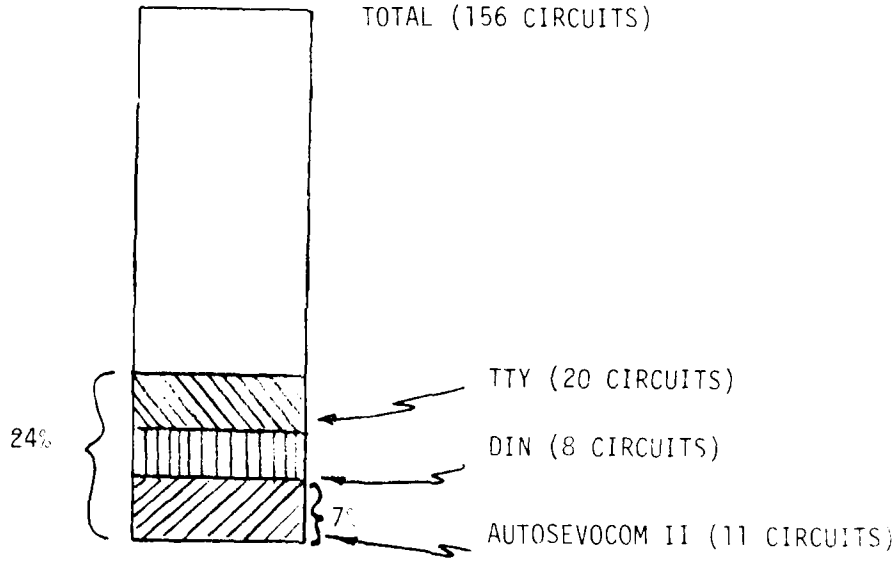


Figure 3-2. Typical Link Cross-Section Distribution Based upon Random Sampling of 15 Links of Projected 1985-1989 Circuit Requirements

c. Digital Interface. Table 3-I summarizes the major switch/transmission characteristics and other considerations affecting the digital interface. Most switches will be configured with one time division matrix (TDMX) with four digital transmission groups, each containing, on the average more than one Inter Switch Trunk (IST). Since the mean switch connectivity requirement exceeds six IST groups there is a definite need to break down and recombine the four digital transmission groups. This is the main task of the interface which will be incorporated at the digital TCF. A summary of the major digital interface requirements is contained in Table 3-II.

2. INTERFACE CONCEPTS

In order to resolve the interface issue, three basic concepts are defined. The first involves integrated interface of analog and digital channels. This concept utilizes nontraditional technology and operations at the TCF. The second concept involves preservation of the traditional configuration and operations of the TCF. Under this concept, two alternatives are evaluated. The last concept involves specialized interface for AUTOSEVOCOM II traffic requiring nontraditional technology and operations at the TCF. Three subalternatives are evaluated for this concept.

a. Concept I. The concept I interface interacts with (1) digitized voice frequency channels at the output of the DRAMA first level multiplexer, and (2) secure voice digital groups and data channels. These digital streams are brought to a common route and format before they are directed to a channel assignment device (i.e., TDMX) which performs channel/group sequence arrangements among the group inputs. The outputs of the channel assignment device (CAD) are 1.544 Mb/s groups which are passed through bulk encryption devices (i.e., KG-81) to the second level multiplexer. Since the CAD addressing can be remotely updated, its useage as a nodal element offers enhanced flexibility and the potential for reduced O&M in the areas of channel/group restoral and reconfiguration. Figure 3-3 depicts the interface functionally. The PCM digroup output streams enter the CAD directly whereas other digital streams are conditioned and multiplexed when necessary, prior to entering the CAD. The figure also shows the percentage of special purpose user traffic and switched traffic within the DCS. Under Concept I, the AUTOSEVOCOM II interface requirements are met as part of achieving an integrated and flexible voice/data channel or group reconfiguration capability.

b. Concept II. This concept utilizes conventional multiplexers to interface AUTOSEVOCOM II channels with the digital transmissions. Two distinct alternatives are shown in Figure 3-4. In alternative 1, the IST digital groups generated by the TTC-39 switch are demultiplexed to 16 kb/s channels. These are then grouped into streams suitable for

TABLE 3-I. MAJOR SWITCH/TRANSMISSION AND OTHER ROUTING CONSIDERATIONS AFFECTING THE DIGITAL INTERFACE

ITC-39 (DIGITAL MATRIX)	First Level MUX (DRAMA)	Other Consideration
digital group rates - 128, 256, 512, 1024, 1536, 2048 kb/s	data interleaving rates - synchronous - 56, 64 128, 256, 512 kb/s - asynchronous - 0-20, 50 kb/s output rate - 1544 kb/s	
channel modularity (16 kb/s) 8, 16, 32, 64, 96, 128	channel modularity (16 kb/s) - data interleaving - 3, 8, 16, 32 max number of channels/level 1 MUX - 48 with any combination of the above channel modularity.	most efficient modularity for spectrum conservation - 3 Channel Grouping
number of transmission digital groups - 4 (1 TDMX Configuration) 150 terminations 8 (2 TDMX Configuration) 300 terminations		max transmission link connectivity - (Europe) 8 Links
maximum number of IST groups - 14 (1 TDMX Configuration) 28 (2 TDMX Configuration)		max switch connectivity - (Europe) 10 IST Groups mean switch connectivity - (Europe) 6.4 IST Groups
framing - CCIS with overhead framing subchannel	framing - PCM/TDM D2/D3 format multiplexing of 16 kb/s requires overhead framing.	
signal interface - conditioned diphase	signal interface - balanced AMI or bipolar	
timing - synchronous, buffers provided, external reference	timing - synchronous, nodal or internal timing reference.	

TABLE 3-II. MAJOR DIGITAL INTERFACE REQUIREMENTS

- AUTOSEVOCOM II trunk routing
- Efficient transmission channel "packing"
- Tech Control functions - channel, group restoral and extension, monitoring, testing and reporting, and responding to higher hierarchical elements.
- SYSCON subchannel (2 kb/s) breakout and routing
- Signal conversion
- Buffering, framing of digital groups

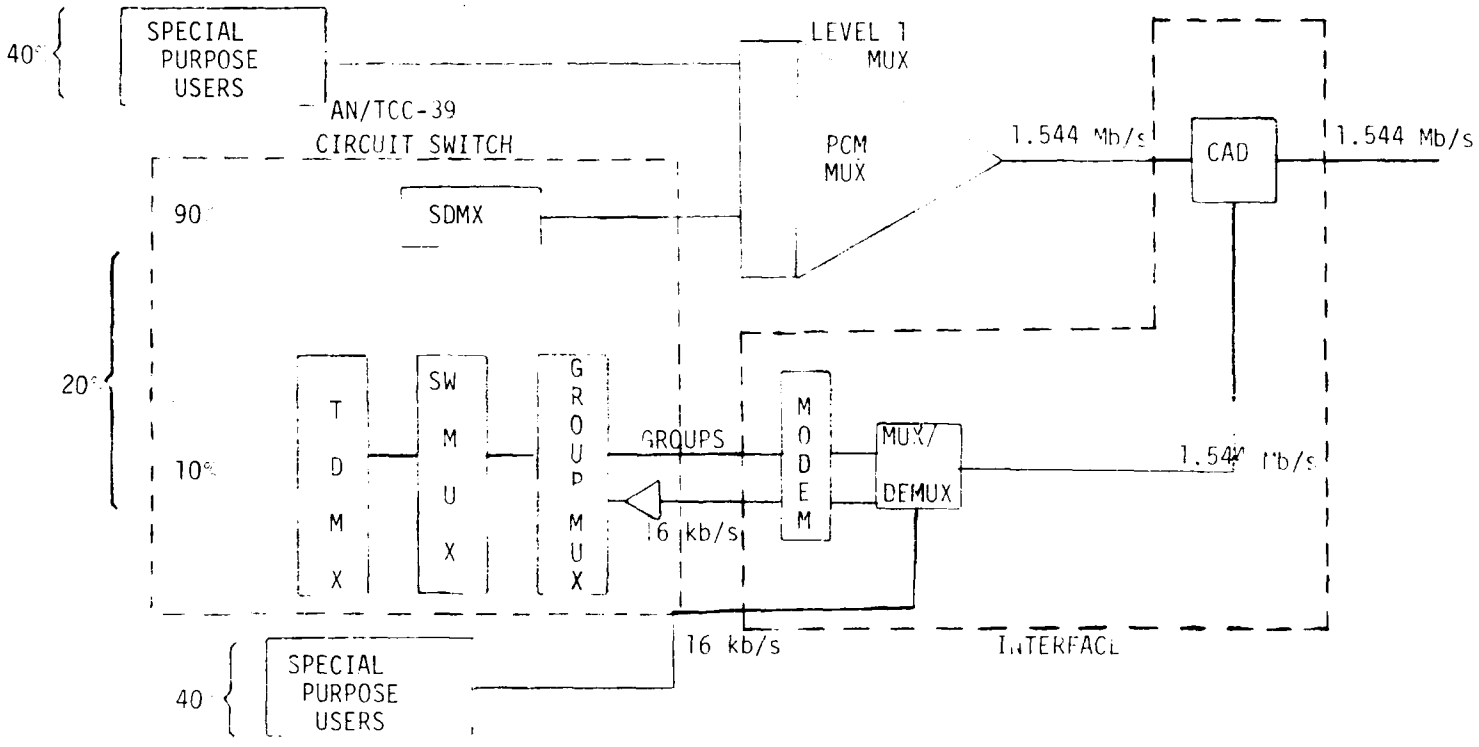


Figure 3-3. CONCEPT I Block Diagram

NOTE: SDMX - SPACE DIVISION MATRIX
TDMX - TIME DIVISION MATRIX

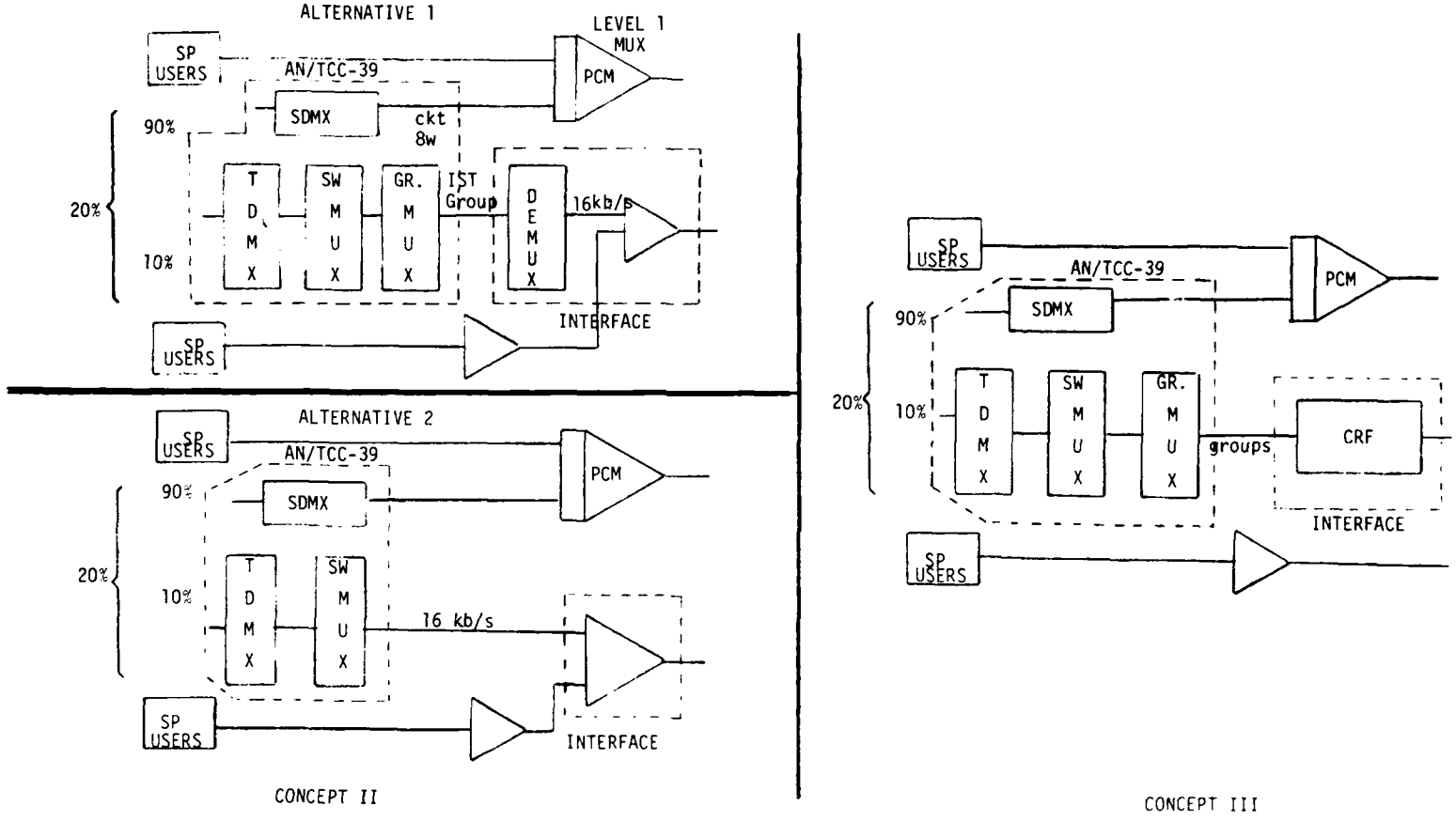


Figure 3-4. CONCEPTS II and III Block Diagram

transmission. Alternative 2 involves the modification of the digital portion of the AN/TTC-39 switch to output 16 kb/s trunks. The function of the interface is to group the channels into streams using conventional multiplexers.

c. Concept III. Concept III employs a channel reassignment function (CRF) device [2]. This device is a programmable multiplexer that essentially utilizes a time division switch matrix to provide AUTOSEVOCOM II connectivity requirements. Functionally, the CRF operates similar to the CAD of Concept I except it interfaces AUTOSEVOCOM II traffic exclusively at rates and formats specified by reference [3]. The outputs of the CRF are routed to the data interleaving ports of the first level PCM multiplexer.

d. Concept Comparison. Table 3-III gives a comparison of the main features of the three concepts. Concept I provides integrated TCF capabilities with the potential for automation and operation and maintenance savings. This concept, however, appears to incur greater initial costs and greater technical and schedule risks and, therefore, is considered not applicable in the near-time frame (i.e., 1980). In the long term, it offers certain subsystem advantages and is being analyzed under DCA study Contract (DCA 100-76-C-0064); it will not be further addressed herein.

Note that all three concepts utilize common channel signaling. This form of IST signaling requires preservation of the prearranged trunk time slot sequence that form the trunk groups so that the location of the overhead (signaling) channels and associated trunks are known at all switches [4]. Changes of the trunk group order at the transmission end must be performed in coordination with the switches affected.

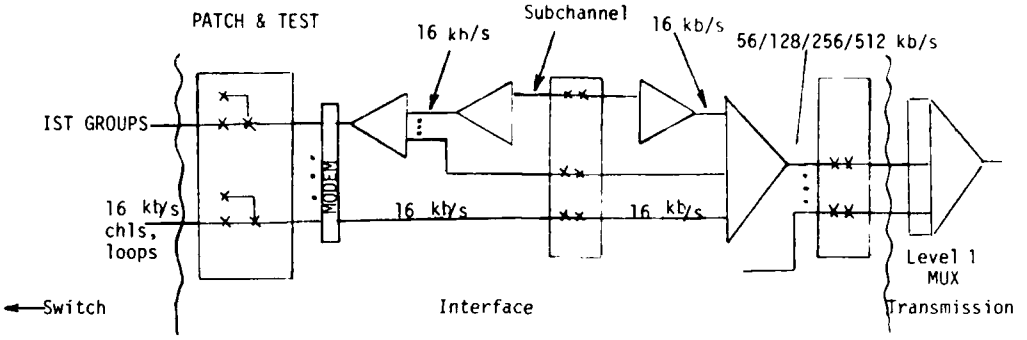
e. Alternative Solutions for Concept II and III. Figure 3-5 shows the solution alternatives for the TCF/Switch/Transmission interfaces. This figure gives a different perspective than Figure 3-4, which serve to accent the interface discussions.

(1) Alternative 1. (Concept II.) IST digital groups are demultiplexed into baseband 16 kb/s channels, and selected overhead channels are broken out to terminate 2 kb/s system control (SYSCON) subchannels. The subchannels are recombined and multiplexed with other 16 kb/s channels to yield digital groups suitable for transmission to other nodal points.

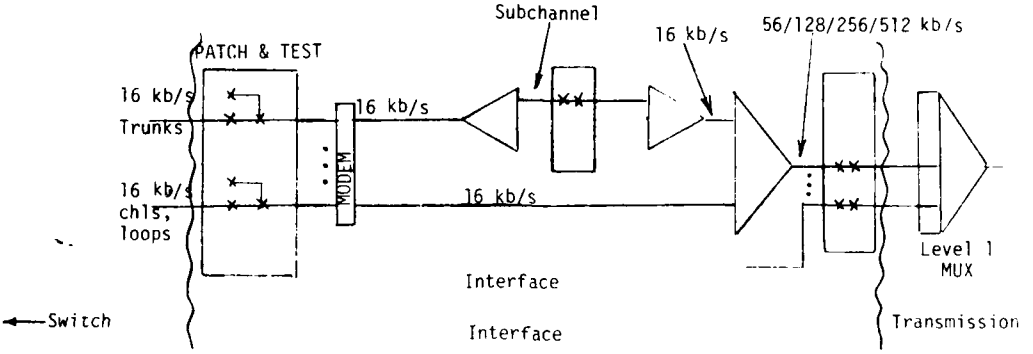
(2) Alternative 2. (Concept II.) AN/TTC-39 switches have been assumed to be modified to output individual 16 kb/s trunks in place of IST groups. In addition to reducing switch equipments such as group multiplexers, framing and buffering elements, this

TABLE [illegible] COMPARISON OF INTERFACE CONCEPTS

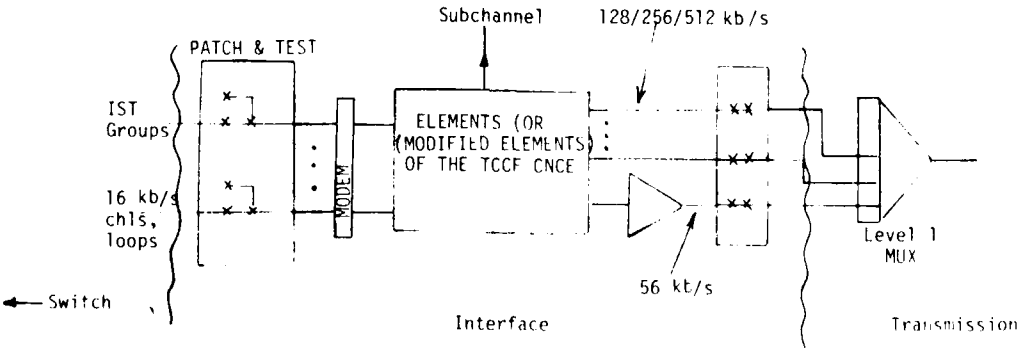
[illegible] I	[illegible] II	[illegible] III
• Interfaces all traffic at the output [illegible] level [illegible] [illegible] [illegible], and special purpose data traffic.	• Interfaces digital AUTOSEVOCOM II 16 kb/s derived traffic.	• Interfaces digital AUTOSEVOCOM II [illegible] traffic.
• Integrated restoral and reconfiguration implementation and operation for all traffic analog & digital.	• Different restoral and reconfiguration, but similar operations for voice, data and AUTOSEVOCOM II secure voice traffic.	• Different restoral and reconfiguration implementation and operations for voice, data, and AUTOSEVOCOM II [illegible] voice traffic.
• Potential for integrated monitoring, testing and fault-isolation implementation.	• Different, monitoring, testing and fault-isolation implementation for voice, data and secure voice traffic.	• Different, monitoring testing, and fault-isolation implementation for voice, data and secure voice traffic.
• Potential for automation of most of the TCF functions.	• Manual operation.	• Automation applies to AUTOSEVOCOM II circuits which are less than 10[illegible] of the total TCF circuit appearances.
• Potential O&M manning level improvement.	• Limited potential for O&M manning level improvement.	• Limited potential for O&M manning level improvement.
• Relatively high technical risk. Requires application of complex hardware. Software necessary to achieve the full potential of the interface is yet to be developed.	• Low technical risk.	• Relatively low technical risk. Hardware [illegible] been developed for [illegible] application. Software requirements have been specified and are being developed.
• Schedule risk [illegible] relatively high. There [illegible] designing the hardware and software [illegible].	• Low schedule risk for 198[illegible] deployment.	• Schedule risk [illegible] under the [illegible] program hardware and software are being developed for 198[illegible] deployment.
• Interface [illegible] assumed relatively high.	• Low implementation cost.	• Cost ranges from low to high depending on the implementation option.



ALTERNATIVE 1 (CONCEPT II)



ALTERNATIVE 2 (CONCEPT II)



ALTERNATIVE 3 (CONCEPT III)

Figure 3-5. AUTOSEVOCOM II Interface Alternatives

alternative results in considerable switch/transmission interface simplification. 16 kb/s overhead channels are demultiplexed to provide SYSCON channel appearance, and then are recombined and multiplexed with other sixteen kb/s channels as in alternative 1.

(3) Alternative 3 (Concept III.) This alternative incorporates modules of the digital elements of the TCCF communications nodal control equipment (CNCE) being developed for the TRI-TAC program. Three subalternative designs, with varying capabilities, complexities, and modifications are given in Figure 3-6. The common element for alternative 3 is the Channel Reassignment Function/Automatic Digital Tester (CRF/ADT). The ADT enables generation and monitoring of digital streams through any selected channel for the purpose of determining average bit error rates. A brief description of the subalternatives is presented below. Detailed discussion is included in a DCEC internal memo [5].

(a) Subalternative 3A. Major digital interface elements of the CNCE (Type III), as specified in reference [6], are considered in this subalternative. Specifically, the processor subsystem, channel reassignment function, ADT visual display unit, hard copier, and a 3-channel submultiplexer for channel packing to 16 kb/s, are considered.

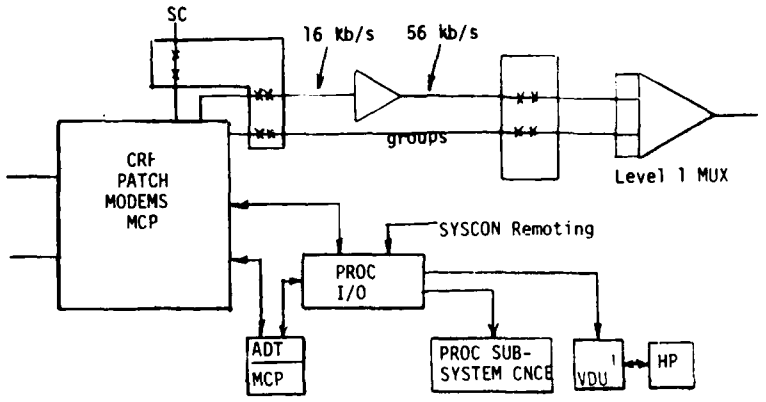
(b) Subalternative 3B. This subalternative uses a microprocessor in place of the CNCE processor subsystem. The remaining elements are identical to those of subalternative A.

(c) Subalternative 3C. This subalternative utilizes the CRF and ADT in the manual mode in a configuration resembling CNCE (Type VI) [6]. The CRF is modified to include the I/O port for possible interface with higher echelon SYSCON elements. No processing or display subsystems are included.

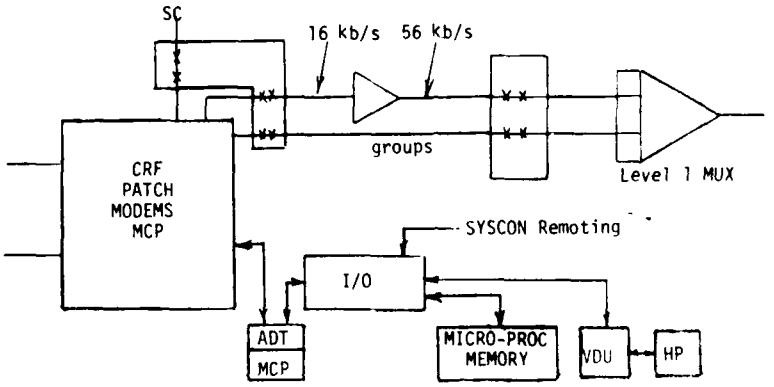
(d) Variations in Alternatives. Certain reasonable variations in each alternative can be described. Since all TCF's will be collocated with switches, the need to deploy modems, both channel and group, to drive digital signals through a cable medium is obviated. Detailed discussion of variations in alternatives is contained in reference [5].

3. ALTERNATIVE EVALUATION

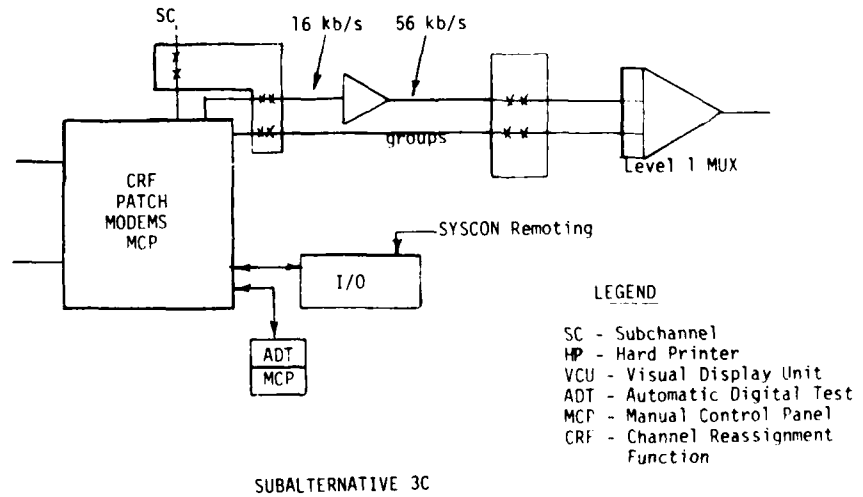
The three alternatives were evaluated using the methodology described in reference [5]. Thirteen possible combinations are ranked in ascending order (i.e., 1-13), 1 being best, and are shown in Table 3-IV. The following discussions provide the rationale for scoring.



SUBALTERNATIVE 3A



SUBALTERNATIVE 3B



SUBALTERNATIVE 3C

Figure 3-6. Subalternatives of Alternative 3

TABLE 3-IV. RANKING OF THE ALTERNATIVES

	ALTERNATIVE	SUBALTERNATIVE	VARIATIONS	Basic Requirement: AUTOSEVOCOM II Interface	Basic Requirement: Transmission Packing	Basic Requirement: SYSCON Subchannel	Syscon Requirement: Automated re-configuration	Syscon Requirement: Automated Testing	Syscon Requirement: Hierarchical Interface	Cost: Switch Nodes	Cost: System (all nodes)	Tech Risk: Hardware	Tech Risk: Software	Schedule Risk	Applicability	O&M: Training	O&M: Operation case	O&M: Manning level	O&M: Potential for remoting	Flexibility: Growth accommodations	Flexibility: Modularity	Maintainability	Communications Availability
Conventional MILV's	1		a	1	1	1	NA	NA	NA	4	2	1	NA	1	1	1	1	1	NA	1	1	1	1
			b	1	1	1				1	1	1	NA	1	1	1	1	1	NA	1	1	1	1
	2		a	1	1	1	NA	NA	NA	5	2	1	NA	3	1	1	1	1	NA	1	1	1	1
			b	1	1	1				1	1	1	NA	3	1	1	1	1	NA	1	1	1	1
CRF	3	A	a	1	2	1	1	1	1	10	11	2	2	2	4	1	1	1	1	1	1	1	1
			b	1	2	1	1	1	1	9	10	2	2	2	4	4	2	1	1	1	1	1	1
			c	1	1	1	1	1	1	8	9	3	2	4	4	4	2	1	1	1	1	4	2
	3	B	a	1	2	1	1	1	1	7	8	4	3	5	3	3	2	1	1	1	1	3	2
			b	1	2	1	1	1	1	6	7	4	3	5	3	3	2	1	1	1	1	3	2
			c	1	1	1	1	1	1	5	6	5	3	6	3	3	2	1	1	1	1	3	2
	3	C	a	1	2	1	2	2	2	5	5	1	NA	2	2	2	3	2	2	1	1	2	3
			b	1	2	1	2	2	2	3	4	1	NA	2	2	2	3	2	2	1	1	2	3
			c	1	1	1	2	2	2	2	3	3	NA	4	2	2	3	2	2	1	1	2	3

a. Basic Requirements. All alternatives were configured to match the AUTOSEVOCOM II interface requirements: routing of IST's, DAX access lines, and loops. They also provide the SYSCON subchannels. Alternative 3, when not configured to generate channel grouping of three 16 kb/s channels, was ranked lower in the area of efficient transmission utilization.

b. Syscon Requirements. Alternative 3 is in general superior in providing semiautomatic means for subchannel, channel, and group configurations. Subalternative 3C was ranked higher than alternatives 1 and 2 on the assumption that the CRF could be easily modified to interface with the higher levels of operational direction.

c. Cost Consideration

(1) Switch Nodal Costs. Figures 3-7 through 3-9 depict the hardware costs versus the total AUTOSEVOCOM II channels at various European switch nodes. The nodal costs, in general, are not simple functions of the numbers of channels, but rather depend on the actual node and switch configurations defined by factors such as: terminating channels and digital groups, local loops, through-groups and branching groups, connectivity, and submultiplexer modularity.

In the cost figures shown, these factors in conjunction with the AUTOSEVOCOM II Network sizing [3] are used to estimate the costs of the switch nodes at sampled DCS locations. These locations include Feldberg, Langerkopf, and Coltano.

Alternative costs at other switch nodes are interpolated, using total number of channels as a parameter, from the estimated costs at the mentioned nodes.

From these figures, subalternative 3A is the most costly and is relatively independent of node size. As the node size decreases, the cost of the other alternatives is reduced.

For all of the alternative variations, b and c appear the most reasonable because the switch and TCF will be collocated. The cost curves for these variations indicate that alternatives 1b, 2b, 3Cb, and 3Cc, which involve manual operation, result in the lowest cost.

The cost estimates are based on data provided by [7], internal memoranda, and reports. No attempt has been made to estimate installation, integration, software, spares, and logistics costs. It is assumed that those factors will further improve alternatives 1, 2, and 3c. The cost impact, incurred from switch modifications, were not evaluated.

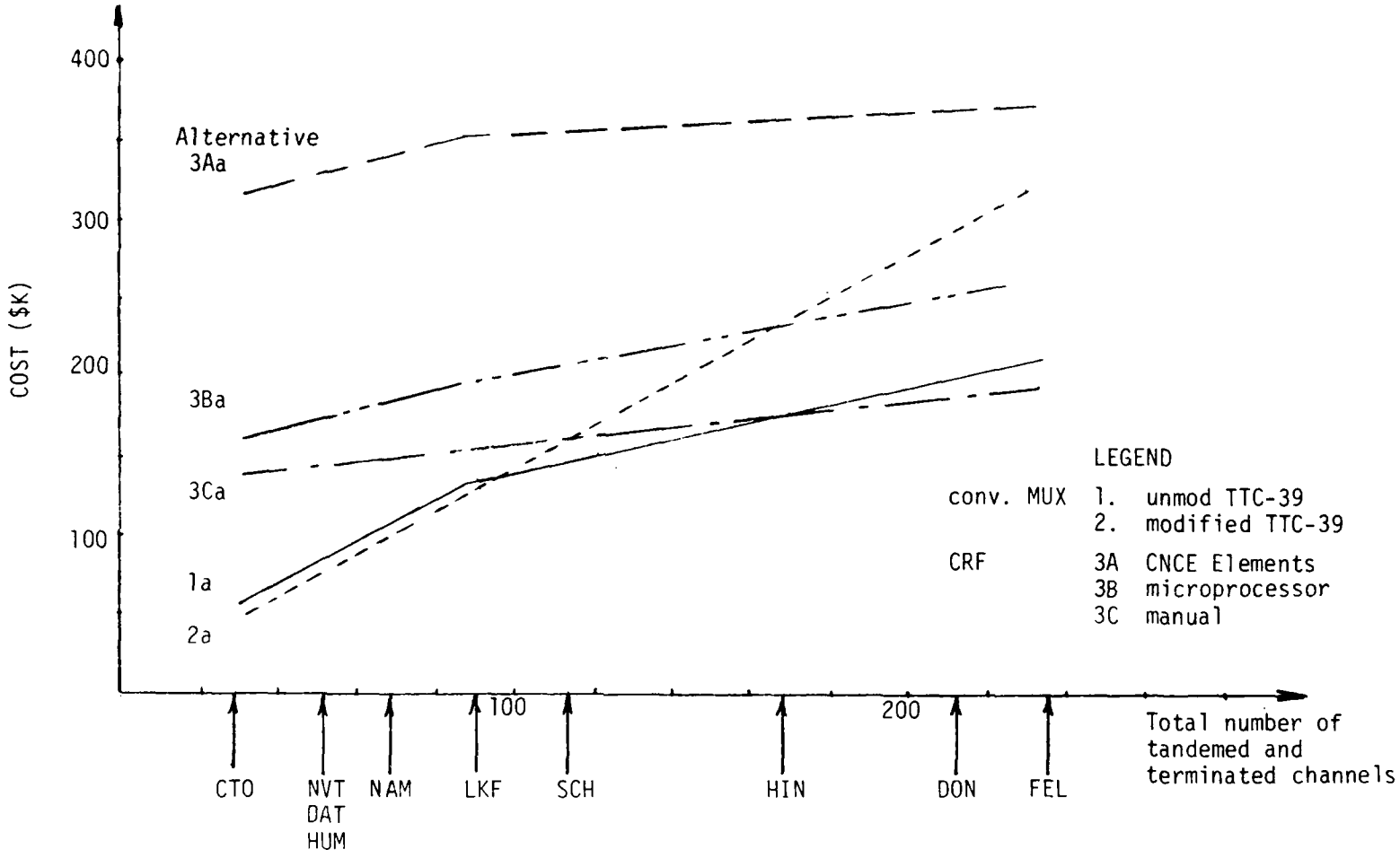


Figure 3-7. Cost vs Total Channels at Switch Nodes - (a) (Modems Included)

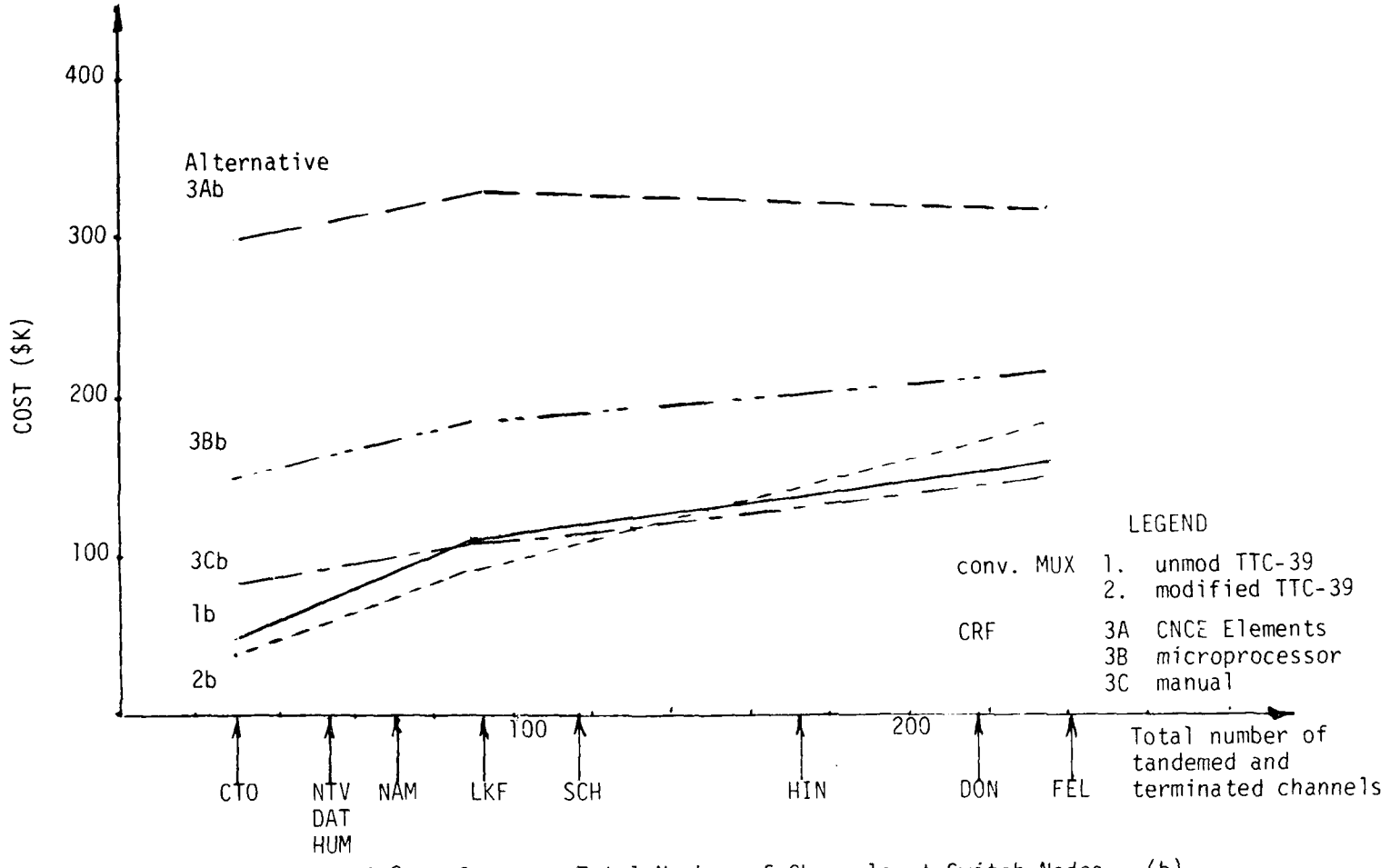


Figure 3-8. Cost vs Total Number of Channels at Switch Nodes - (b)
(Switch -TCF Collocated/Group Modems Excluded)

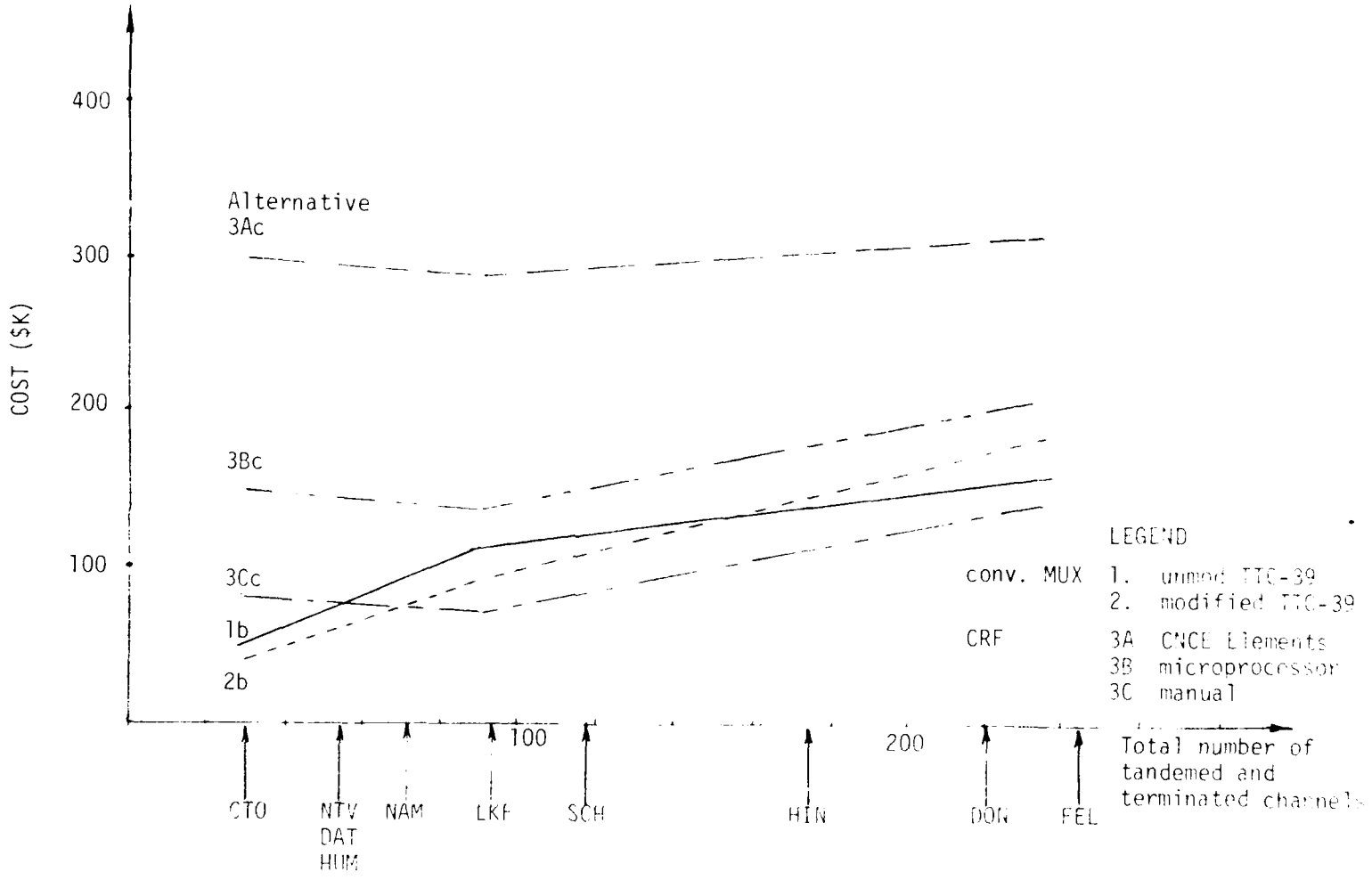


Figure 3-9. Cost vs Total Number of Channels at Switch Nodes - (c)
(Switch -TCF Collocated; CRF modified/Group Modem Excluded)

(2) System Costs. The majority of DCS nodes currently are obviously not switched nodes. Most nodes serve mainly as drop and insert or through-group and branching nodes. Figure 3-10 provides a histogram of projected European AUTOSEVOCOM II DAX trunks, which is based on a specific network sizing [3]. The alternative costs associated with DAX nodes, direct homed subscriber drop and insert nodes, and through-group and branching nodes are shown in Figure 3-11. It is apparent that from the system cost view, alternatives 1 and 2 are better than alternative 3.

d. Technical Risks. The multiplexers considered in alternatives 1 and 2 are noninventory items. However, similar hardware being developed under the TRI-TAC program, is characterized by off-the-shelf technology and known design techniques. Therefore, these alternatives are ranked as high as 3Ca and 3Cb, which have been developed. The remaining alternatives involve changes to specification, software development, or new design, and thus have a higher risk.

e. Schedule Risk. Only alternatives 3A (a,b), 3C (a,b) are currently programmed for development and deployment (TCCF program). A slip in the program due to problems on CNCE software development will affect the 1980 production objective. Alternative 1, if programmed within a year should not result in schedule risk. Alternative 2 involves specification change in the TTC-39 switch, and therefore may incur considerable schedule risks. The remaining alternatives involve various modifications in software, hardware, and therefore high schedule risk.

f. Applicability. This criterion ranks the applicability of each interface alternative to the various DCS nodes. Based upon costs and risks factors, alternatives 1 and 2 were evaluated to be best. A hybrid alternative employing CRF at switch nodes and conventional multiplexers at other nodes is also possible. The cost of this configuration will be substantially lower than that of the "pure" CRF alternatives, but higher than the "pure" multiplexer alternative.

g. O&M. Training in new skills, operational familiarity, and ease of operation favors alternatives 1 and 2. The operational manning level required is assessed to be about the same for all alternatives, with the possible exception of alternative 3C where the operational complexity may increase personnel level. Alternatives employing CRF have potential for future remote operation.

h. Flexibility. All alternatives are modular and will accommodate growth or changes in AUTOSEVOCOM nodal traffic.

i. Maintainability. This criterion is primarily a function of the equipment complexity and sophistication; consequently, alternatives

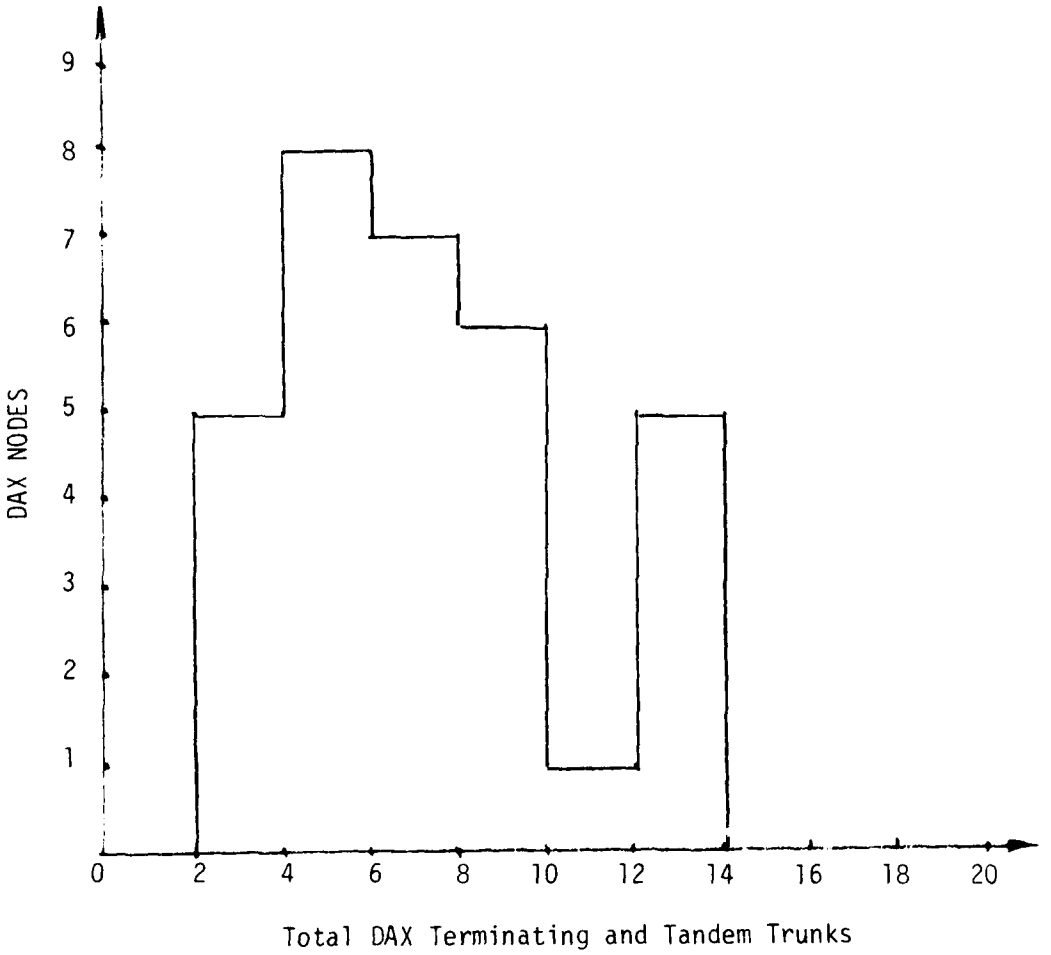


Figure 3-10. Histogram of the Number of DAX Nodes vs the Total Number of DAX Trunks

LEGEND

1,2 - conventional MUX
3A - TCCF/CNCE modules
3B - CRF with microprocessor
3C - manual CRF

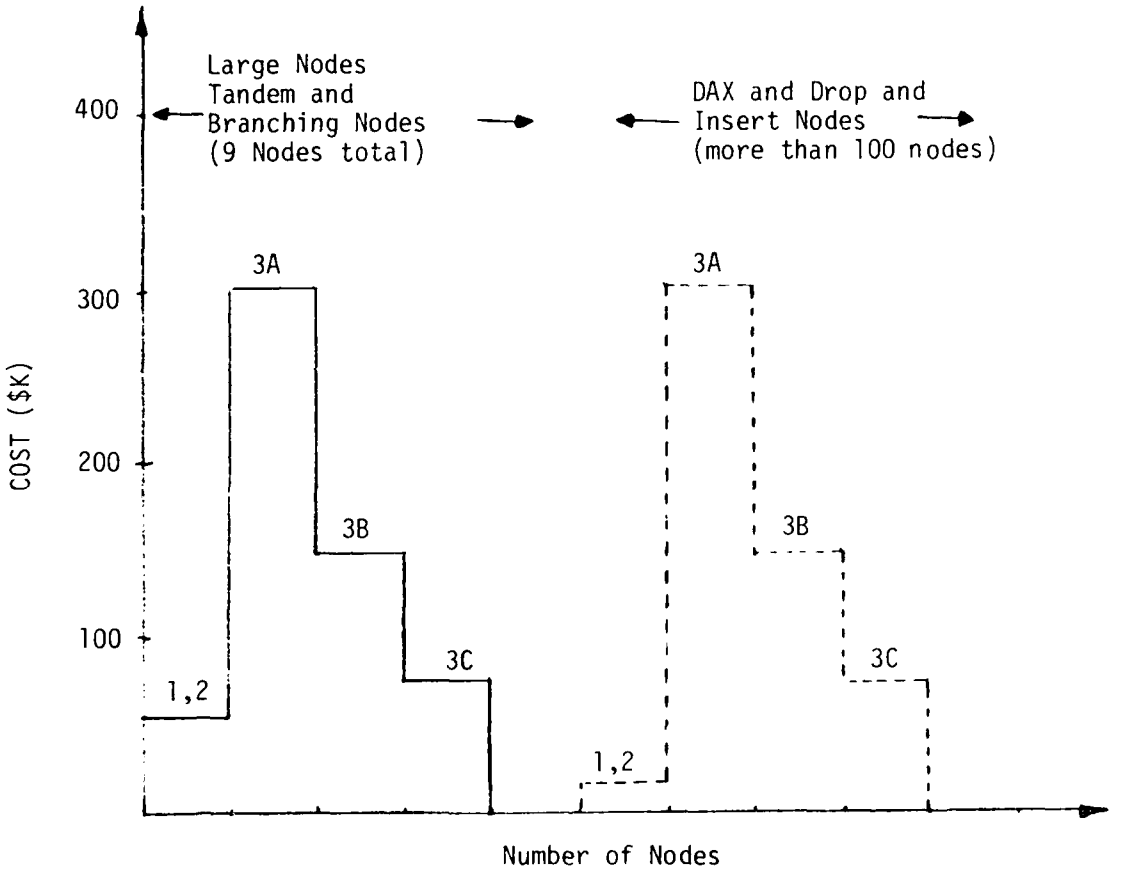


Figure 3-11. Cost of Typical Nodes as a Function of the Number of Nodes

1 and 2 rank the highest. Alternative 3 which is, in effect, a time division matrix would require specially trained personnel to maintain the software (3A and 3B) and the relatively complex hardware.

j. Communications Availability. Failure of a given multiplexer results in outage of channels associated with that particular multiplexer. Failure of the CRF memory results in total nodal channel outage. In short, given the same fault conditions, alternatives 1 and 2 involve "graceful" degradation, whereas alternative 3 may result in total outage.

IV. TRANSMISSION DIGITIZATION STRATEGY

This issue is concerned with achieving a viable strategy for digitizing predominately analog DCS traffic as the DCS transitions to an all-digital system. As such, it has significant implications with respect to frequency spectrum utilization and ease of transition. Background information is provided on commercial, current DCS, and transitional DCS digitization considerations. Traffic growth projections are presented to indicate the percentages of traffic that can be expected to be digital and to indicate the relative percentages of terminals that will not originate digital traffic. The framework is then provided in which the digitization alternatives are discussed. A comparison of certain A/D techniques is presented and their application in the transitional DCS is discussed.

1. DIGITIZATION CONSIDERATIONS

The digitization strategy for the DCS (non-AUTOSEVOCOM) has been based on the conversion of 4 kHz analog voice channels to 64 kb/s pulse code modulation (PCM) digital channels [8]. This technique was chosen because it is proven [9], and because it meets the DCS performance requirements imposed by the existing analog plant, the more important of which are: tandeming (i.e., multiple analog-to-digital (A/D) and D/A conversions) and the ability to convert quasi-analog signals to a digital format [8].

However, it appears that this digitization technique is bandwidth inefficient as compared to other A/D techniques, in that one 4 kHz voice channel requires 64 kb/s. This bandwidth problem raises questions of spectrum utilization stemming primarily from DCS frequency and bandwidth allocations in Europe. For example, given a 14 MHz bandwidth, it is possible to obtain approximately 600 4 kHz channels using FDM/FM techniques; whereas, using 64 kb/s PCM, only 192 equivalent 4 kHz voice channels are possible for the same 14 MHz bandwidth as implemented in the FKV program [10].

To alleviate this problem, another possible digitization strategy has been proposed. This is the use of delta modulation (DM) for improved coding of voice. Compared to 64 kb/s PCM, an improvement in the voice handling capacity of transmission equipments by a factor of approximately two is possible with DM at 32 kb/s. However, it does not have the "drop-in" adequacy that PCM has in the analog plant.

The trend toward PCM has evolved primarily because of its complete transparency to all analog traffic, a factor which influenced AT&T's digital growth strategy centered around 64 kb/s. Also,

European common carriers have conceptualized systems based on 64 kb/s derived channels. However, there is also a trend toward DM as exhibited by the availability of DM multiplex equipment from European manufacturers and its use as a voice encoding scheme in the TRI-TAC program, EUROCOM program, Phase II secure voice, etc.

a. Commercial. Commercial equipment is available today which employs 64 kb/s PCM (e.g., AT&T's T-carrier system). Likewise, 32 kb/s DM, the Phillips Type 8TR610 DELTAMUX, and similar equipments produced by Siemens, Marconi, and Ericson, are commercially available.

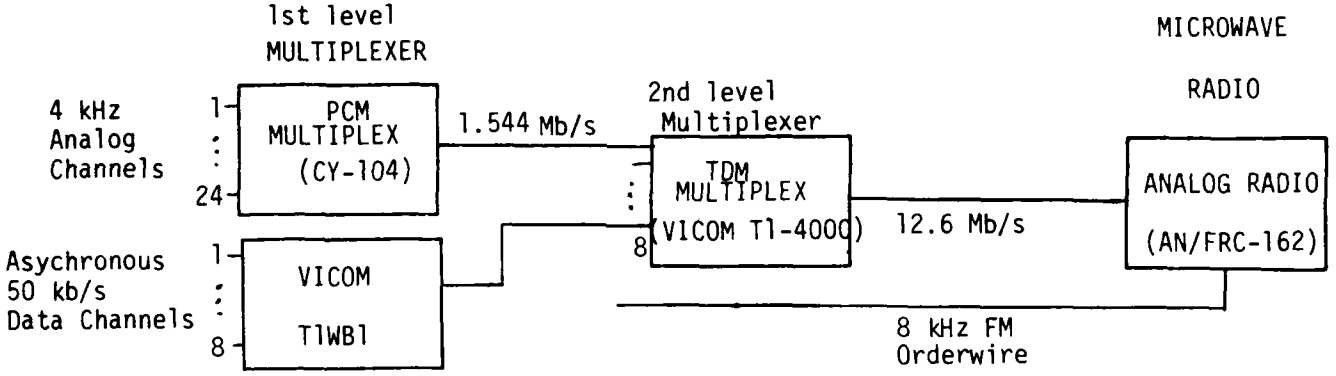
b. Current DCS Digitization. The initial upgrade of the DCS transmission plant has replaced analog (FDM) derived 4 kHz channels with digital 64 kb/s PCM channels accompanied by specific changes in network sizing to accommodate current and projected near-term requirements. The FKV transmission system upgrade program [10] is presently operating on a PCM/TDM/FM hierarchy, with bulk encryption; high-speed data traffic, and digital voice traffic are passed over the system. This hierarchy is shown in Figure 4-1.

c. DCS Transition. The transition of DCS transmission from analog to digital is planned to be accomplished principally with equipment to be procured for the Digital Radio and Multiplex Acquisition (DRAMA) transmission subsystem. The primary multiplex equipment will utilize 64 kb/s PCM. It will also have the capability to accept digital signals directly.

2. OVERSEAS TRAFFIC GROWTH PROJECTIONS

The bulk of present DCS service is devoted to 4 kHz analog voice. Digital service is provided by the present AUTODIN I system. Table 4-I shows the percentage of DCS circuits utilized to provide the listed services based upon the modulation rate carried within the European and Pacific areas. Typical link cross-sections based on random samples from both the European and Pacific areas are given in Table 4-II. This table highlights the analog nature of the DCS.

a. European. Currently, 17% of the average terrestrial analog link channel capacity is devoted to carrying digital traffic in Europe. Projections indicate that this may reach 25% in the mid-1980's. This fact has not, of itself, become the motivating factor for digitization. Rather, the primary motivation is to satisfy certain program requirements for AUTOSEVOCOM II, AUTODIN, and the DSCS that will be appearing in the early 1980's, and to allow for backbone network encryption. Based on current major DCS program plans, traffic projections for clear and secure voice, data, and narrative/record service are given in Table 4-III. As seen from Figure 4-2, by 1988 approximately 61% of the DCS European transmission plant will be digital.



Transmission Characteristics

RF Bandwidth	Number of 64 kb/s Channels
14 MHz	192

Figure 4-1. FKV Configuration

TABLE 4-I. PERCENTAGE OF DCS CIRCUIT CAPACITY UTILIZED TO PROVIDE VARIOUS SERVICES

	EUROPE (%)	PACIFIC (%)
Analog Voice	72.6	77.5
Quasi-Analog		
Low Speed Data	15.2	13.6
Medium Speed Data	5.3	3.7
High Speed Data	.5	.5
Facsimile	.2	.2
CW	.2	.1
Multiplexed Data/Secure Voice	2.4	.8
Speech Plus/VFCT	.6	3.5

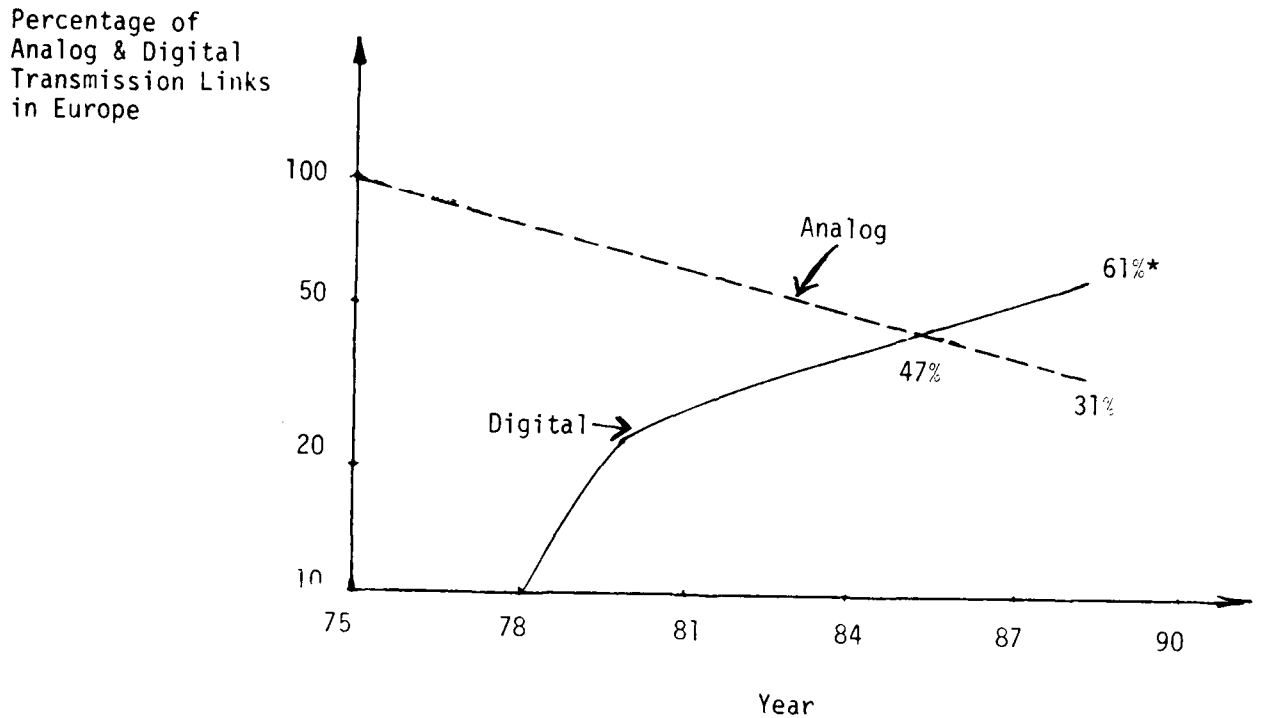
TABLE 4-II. TYPICAL DCS LINK CROSS-SECTIONS BASED ON 35 RANDOM SAMPLES FROM EACH AREA

		NUMBER OF CIRCUITS	
		Europe	Pacific
Analog			
Voice	Nominal 3 kHz	119	107
Facsimile	120 Scan	1	1
Speech Plus	1 Voice & 2 TTY	3	3
Digital			
AUTODIN	2400 b/s	2	2
Teletype	<34 baud	1	1
	45.5 baud	3	2
	50 baud	2	1
	61.12 baud	8	8
	74.2 baud	3	6
	75.0 baud	8	7
Medium Speed Data	150 baud	2	1
	300 baud	2	1
	600 baud	1	0
	1200 baud	3	2
	2400 baud	2	2
VFCT	12 TTY @ 2.4 kb/s	3	3
Multiplexed Data/Secure Voice	2400 b/s	3	2
	4800 b/s	1	0
	9600 b/s	0	1

TABLE 4-III. EUROPEAN GROWTH TRENDS*

Clear Voice	Current	Projected (1988)
Erlangs of Traffic/busy hours	910	1700**
Interswitch Trunks	1100	2100**
Access Lines	2100	4100**
Subscriber terminals	70000	110,000**
AUTODIN		
Narrative/Record (bits/day)	1.79×10^8	2.64×10^8
Pattern, Bulk, Interactive Data (bits/day)	4.19×10^8	3.36×10^{10}
Terminals	220 (AUTODIN I)	660 (AUTODIN II)
Secure Voice		
Erlangs of Traffic/busy hour	18	88
Subscriber Terminals	242	948

*Based on current program plans and bit rates therein associated.
**Includes European Telephone System (ETS) Network.



*Approximately 8% of current analog links are deactivated by 1988 and not replaced by digital links.

Figure 4-2. Percentage of Analog and Digital Transmission Links in Europe

However, as can be seen from Table 4-III less than 10% of the total traffic erlangs introduced into the system will have originated from digital terminals. The projections given assume no major perturbations and that there is no pressure to convert clear voice terminals to digital operation.

b. Pacific. Of the average terrestrial analog link capacity, 14% is devoted to carrying digital traffic in the Pacific. As in Europe, the motivating factor for digitization is the need to satisfy near-term program plans and to allow backbone encryption. Based on current major DCS program plans, traffic projections for clear and secure voice, data, and narrative/record services are given in Table 4-IV. As seen from Figure 4-3, by 1988 approximately 80% of the DCS Pacific transmission plant will be digital. However, less than 15% of the total erlangs of traffic introduced into the system will have originated from digital terminals [11]. Again, no major perturbations or pressures to convert from analog to digital terminals are assumed. As may be seen from these tables and figures, DCS digitization will be heavily concentrated in the backbone network rather than in the access area, with the exception of the AUTOSEVOCOM II program, which will employ a 100% digital secure voice strategy.

3. DIGITIZATION STRATEGIES

The traffic projections presented, together with the percentages of digitization, provide a measure for understanding digitization alternatives.

The alternatives for digitization discussed below are not concerned with a strategy for digital conversion of clear voice and modem derived data from their present analog state. Rather, the alternatives treat A/D conversion in the DCS transmission subsystem only. Of importance, however, is the application of these alternatives to communities of clear voice subscribers, specifically, clear voice AUTOVON and the European Telephone System.

a. Alternative 1. This alternative addresses the currently planned 64 kb/s PCM/TDM digitization strategy. Figure 4-4 presents a simple view of this alternative. The PCM multiplex will accept up to twenty four 4 kHz analog voice channels and output a 1.544 Mb/s data stream to the second level MUX. It will be possible to replace up to 12 voice channels in each digroup with digital data channels of any of the following types:

TABLE 4-IV. PACIFIC GROWTH TRENDS*

Clear Voice	Current	Projected (1988)
Erlangs of Traffic/busy hours	780	990
Interswitch trunks	948	1200
Access Lines	1800	2300
Subscriber Terminals	60,000	60,000
AUTODIN		
Narrative/Record (bits/day)	2.44×10^8	[illegible]
Pattern, Bulk, Interactive Data (bits/day)	5.71×10^8	[illegible]
Terminals	300 (AUTODIN I)	[illegible] (AUTODIN II)
Secure Voice		
Erlangs of traffic/busy hours	23	[illegible]
Subscriber Terminals	317	[illegible]

*Based on current program plans and bit rates therein associated.

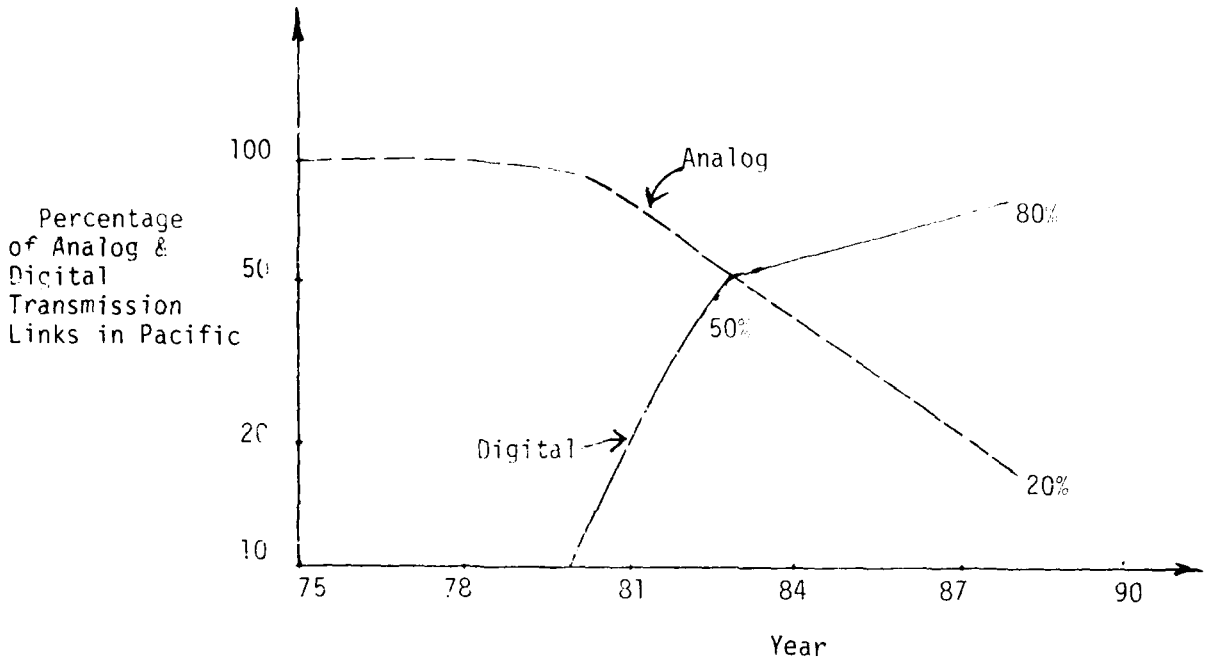


Figure 4-3. Percentage of Analog and Digital Transmission Links in the Pacific

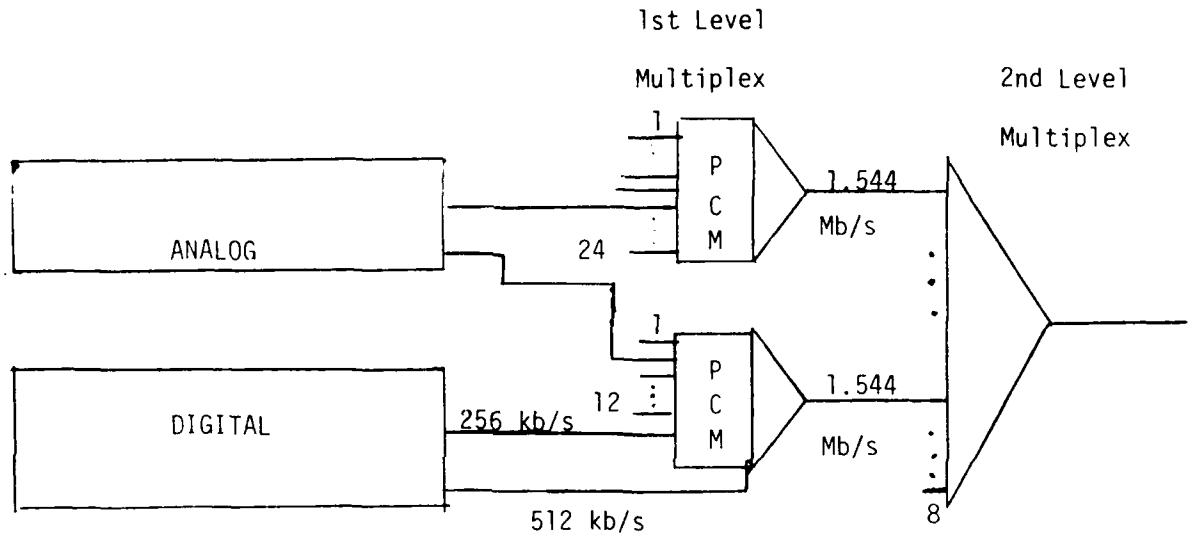


Figure 4-4. Alternative I

(1) 50 kb/s asynchronous

(2) 56 or 64 kb/s synchronous

(3) 128, 256 or 512 kb/s synchronous

(4) 0-20 kb/s asynchronous.

Each channel of the above data sources except (3) shall displace one voice channel. Each 128, 256, or 512 kb/s data channel shall displace two, four, or eight voice channels respectively.

b. Alternative II. Figure 4-5 shows a simple breakout of this alternative. It is characterized by the same 24 channel PCM MUX as in alternative 1. However, a DM MUX in the form of continuous variable-slope delta (CVSD) modulation has been added which will accept up to forty five 4 kHz analog voice channels and output a 1.544 Mb/s data stream. This stream will comprise forty five 32 kb/s data streams plus overhead to build up to 1.544 Mb/s. The CVSD MUX will be used strictly for clear voice A/D conversion because it is known that CVSD cannot accommodate the variety of quasi-analog signals expected in the DCS. Signaling and supervision signals are not passed through the CVSD circuitry of the MUX, but rather are detected and then converted by separate circuitry.

This alternative has the advantage of employing DM at a lower basic bit rate than PCM, and hence can make for more efficient use of available bandwidth than alternative 1. This point becomes more pronounced if the CVSD conversion rate is halved to 16 kb/s, so that 90 channels could be accommodated.

4. COMPARISON OF DM AND PCM

The salient differences between 64 kb/s PCM and 32 kb/s DM are depicted in Table 4-V. Because 32 kb/s DM approximately doubles the channel capacity of 64 kb/s PCM, DM is more bandwidth efficient than PCM.

In some respects, the DM coder is easier to implement and therefore potentially less costly than the PCM coder. This arises because no expensive filters with steep slopes are required and the DM has many building blocks which are identical. The DM encoder is also simpler because it does not require the word synchronization which is necessary for PCM. In the 1960's, the advantage of PCM was that a coder could be shared; however, today more PCM multiplexers are using a single encoder per channel to avoid analog cross talk involved in switching the PCM encoder between channels.

The effect of channel errors upon PCM is more severe than DM because there is a hierarchy to the transmitted PCM signal; i.e., an

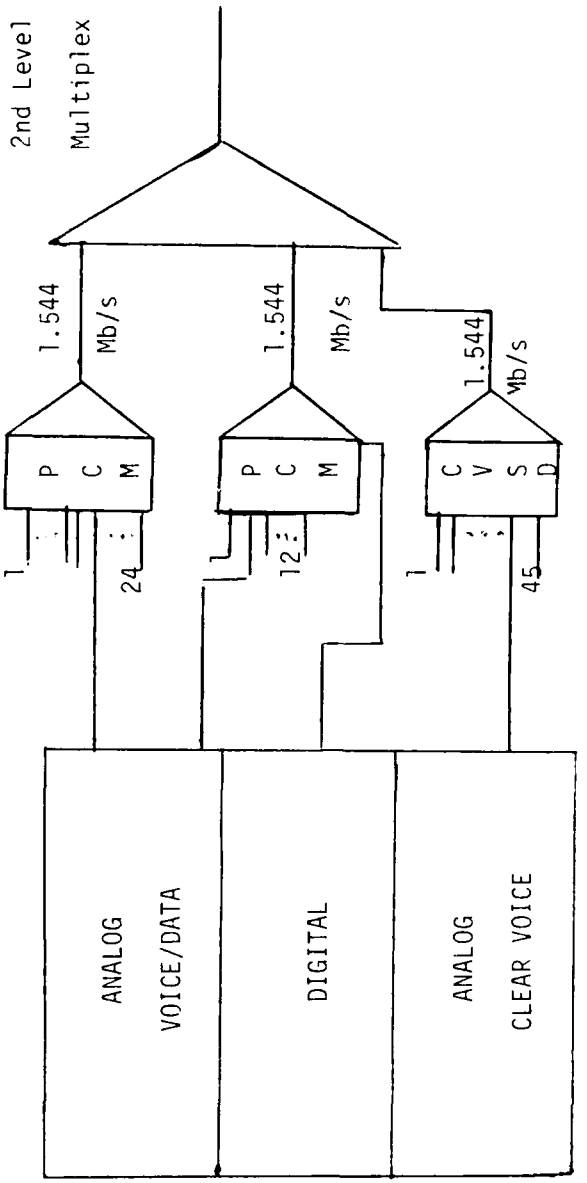


Figure 4-5. ALTERNATIVE Ii

TABLE 4-V. COMPARISON OF 64 kb/s PCM AND 32 kb/s DM

32 kb/s DM	64 kb/s PCM
• ≈ 2:1 increase in channel capacity	• Bandwith inefficient
• Encoder less complex and potentially less expensive	• Encoder requires expensive filters with steep slopes
• Channel errors less severe	• Performs worse in high channel error environment
• Suffers degradation through multiple A to D, D to A conversions	• Transparent (i.e., can be "dropped into") an analog communication system with little or no ill effects.
• Distortion of quasi-analog signals especially above 2 kHz	

error in the most significant bit of a PCM codeword can lead to an error as great as 2^n quantization levels. Even worse, word synchronization can be lost with PCM.

The main advantage of 64 kb/s PCM is that it can be incorporated into a 4 kHz analog communications system with little or no adverse effect; i.e., it can pass analog voice as well as quasi-analog signals through many A-to-D and D-to-A tandem conversions. On the other hand, DM is limited to a range of 4 to 8 A to D and D to A conversions and is also limited with respect to quasi-analog signals, especially those above 2 kHz.

5. APPLICATION OF DM TO THE DCS IN EUROPE

Table 4-III projects that by 1988 clear voice traffic in Europe, including clear voice AUTOVON and ETS traffic, will increase significantly. This is important when considering possible traffic classes that may be included in the digital transmission subsystem, in terms of the mentioned alternatives.

It is known that PCM in alternative I will accommodate these classes of analog traffic and any quasi-analog signal traffic, bandlimited to 4 KHz. However, the DCS is experiencing difficulty in obtaining the required bandwidth to support digital traffic. Spectrum efficiency is therefore of utmost importance.

The application of a DM multiplex to the transmission subsystem, alternative II, has spectrum efficiencies when compared to PCM. Since DM does not handle quasi-analog traffic satisfactorily, it is suggested that DM could be used for clear voice subscribers only. The problems of signaling and supervision over voice networks can be accommodated using commercially available signal converters.

Hence, both clear voice AUTOVON and ETS traffic appear to be excellent candidates for DM at 32 kb/s, particularly when used under short tandem conditions. Furthermore, both systems are located in a region where frequency allocation problems persist (i.e., Europe). To quantify this, the baseline DCS, circa 1980, as defined in the Mix of Media Study [12] was analyzed. The results of this analysis are given in Figure 4-6, which shows the average percentage increase in available channels for 48, 96, 144, 194, 288, and 384 channel digital radio links in Germany when converted from 64 kb/s PCM to 32 kb/s DM. The percentage increase is considered to be a best estimate, as efficient multiplex grouping is assumed. The links of primary importance are the 288 and 384 channel systems, since they require bandwidths in excess of 7 MHz. In order to achieve a significant bandwidth reduction for these links, (i.e., from 14 MHz to 7 MHz), the number of 64 kb/s channels required would have to be reduced

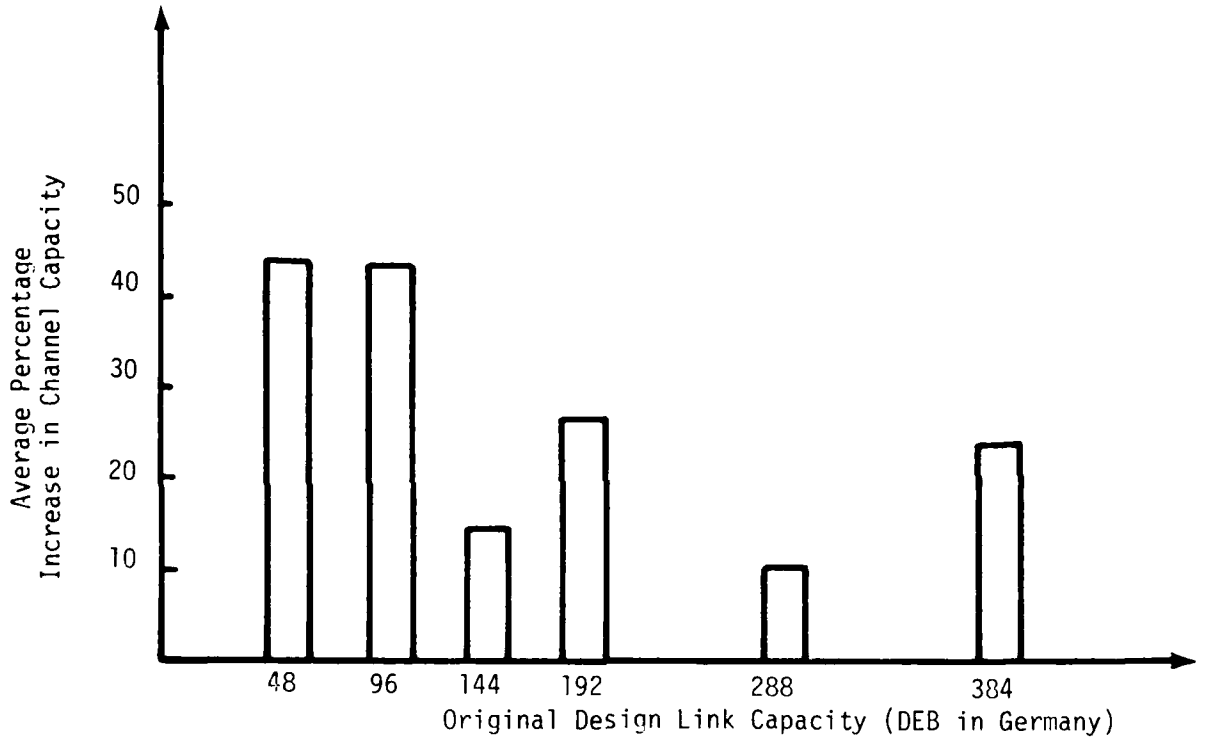


Figure 4-6. Potential Increase in Channel Capacity of Digital European Backbone by Conversion of 64 kb/s PCM to 32 kb/s DM

by approximately 25% for the 288 channel links and 50% for the 384 channel links. Of the 384 channel links (22 in Germany), the highest channel reduction achieved, using 32 kb/s DM, was about 39%. This was for the Donnersberg-Sembach link. Of the 288 channel links (14 in Germany), only two showed a significant bandwidth reduction. These were the Schwanberg-Wurzburg and the Brandhof-Nuernberg links. On the basis of these results, 32 kb/s DM would not significantly reduce the bandwidth requirements in Europe, but it would increase channel capacity by 15-25%. An additional analysis including all clear voice traffic, along with ETS and AUTOVON, did not show a significant change in the results.

An additional application for DM at 32 kb/s is increasing the capacity of leased DCS transoceanic IST's. Here, the payoff is a clear doubling of the channel capacity as compared to 64 kb/s PCM. However, because DM might not pass certain quasi-analog traffic, particularly high speed data at 9.6 kb/s and some medium speed data at 4.8 kb/s, certain provisions for these traffic types would be necessary.

6. ASSESSMENT OF ALTERNATIVES

Both digitization alternative I, PCM, and digitization alternative II, PCM and DM, have certain advantages and disadvantages which have been evaluated. To assess the effectiveness of each alternative, a set of measures of effectiveness (MOE) was devised. Each measure is assigned a weight based upon its estimated importance to the DCS. Each alternative is then given a rank for each MOE based upon the analyses as described below. Finally, a figure of merit was obtained for each alternative by summing the weight and rank for each MOE.

a. Bandwidth Reduction. This measure considers the bandwidth reduction that may be possible by using more efficient A/D techniques. It has been shown that the use of 32 kb/s delta modulation for certain clear voice DCS subscribers in Europe would not result in significantly lower bandwidth requirements over 64 kb/s PCM for the DEB. Each alternative is then given an equally low rating.

b. Capacity. This measure of effectiveness evaluates the potential increase in capacity or growth that one alternative has over the other. As has been discussed, alternative II has a higher channel capacity than alternative I because approximately two 32 kb/s DM voice channels can replace one 64 kb/s PCM voice channel.

c. Ease of Through-Grouping. This is a measure of the efficiency of the multiplex equipment in reducing the number of conversions to the baseband level. Alternative I is better in that all traffic will be converted to 64 kb/s PCM and multiplexed in 24

channel groups. Conversely, alternative II does not lend itself to ease of through-grouping because of the additional multiplex equipment required for DM. The DM multiplex will group 45 channels at an output rate of 1.544 Mb/s. Other lower order DM MUX's will be required for group modularities less than 45 channels, thus further complicating the multiplex hierarchy.

d. Ease of Transition. In the near term (early 1980's), PCM is superior to DM in that it can be placed in an analog system and appear transparent to all the various types of traffic being transmitted through the system. This is not true of DM.

In the far term (late 1980's), as more of the DCS assets become digital, DM will prove to be more advantageous then PCM because of its higher capacity.

e. Tandem Performance. This is a measure of the system's ability to transfer information from one subscriber to another without introducing appreciable errors. For previous analyses it was assumed that the transmission media and switching equipment would introduce an error rate which remains constant for both alternatives. Alternative I would introduce the least signal degradation in a tandem A/D environment.

f. Technical Risk. Complexity of new developments and hardware modifications is next considered. Both alternatives are rated equal in this regard, as equipment has been developed by commercial manufacturers which can be used, with slight modifications, in the DCS.

g. Cost. This measure considers the cost of equipment developments and modifications as well as that of logistical support factors. Since alternative II involves the modification of more equipment than alternative I, it will have a higher development cost and may have a higher logistics support cost.

h. Security. Because DM has a higher capacity then PCM, more subscribers can be converted to digital, which in turn can be encrypted. Hence, DM has a higher potential than PCM with respect to providing security.

i. Maintainability. The ability to detect and correct failures in a given alternative equipment configuration constitutes this measure. Maintainability is primarily a function of equipment complexity and sophistication. Alternative II will be more difficult to maintain than alternative I because of the additional DM multiplex equipment.

j. Survivability. The ability of equipment to perform in a degraded mode as might be associated with a war-time environment,

particularly nuclear conflict, has a direct impact on system survivability. The increased channel capacity provided by DM and its higher tolerance to transmission errors than PCM would allow a more graceful system degradation as the amount of traffic increases, due to circuit rerouting around the damaged parts of the system.

k. Manpower Skill Level. This measure is concerned with the number and skill level of personnel required to operate and maintain equipment associated with each alternative. This measure is also primarily a function of equipment complexity and sophistication. Alternative I would have the lowest manpower requirements because no additional O&M personnel are involved. Alternative II,while probably not requiring additional personnel, would require some additional training for the DM equipment. Therefore, alternative I is given a higher rating than alternative II.

7. SUMMARY OF ASSESSMENT

The results of each assessment category have been summarized in the Table 4-VI along with the calculation of an overall figure of merit for each alternative. It was found that alternative I, the PCM digitization strategy, has a higher figure of merit than alternative II, the combined PCM, DM alternative. In the future, however, the advantages of DM may outweigh those of PCM, especially as the DCS employs more digital transmission and switching.

TABLE 4-VI. ASSESSMENT OF ALTERNATIVES WITH FIGURE OF MERIT

MEASURE	WEIGHT	RANK OF ALTERNATIVE		WEIGHT X RANK	
		ALT 1	ALT 2	ALT 1	ALT 2
BANDWIDTH REDUCTION	10	1	1	10	10
CAPACITY	10	1	2	10	20
EASE OF THRU-GROUP	8	2	1	16	8
EASE OF TRANSITION:					
NEAR TERM	8	2	1	16	8
FAR TERM	6	1	2	6	12
TANDEM PERFORMANCE	8	2	1	16	8
TECHNICAL RISK	7	2	2	14	14
COST	7	2	1	14	7
SECURITY	5	1	2	5	10
MAINTAINABILITY	4	2	1	8	4
SURVIVABILITY	4	1	2	4	8
MANPOWER SKILL LEVEL	2	2	1	4	2
			TOTAL	123	107

V. DCS ENCRYPTION

To secure sensitive information transmitted in the DCS, encryption of lines and trunks, in both backbone and access areas, can be expected. The backbone network will be encrypted in conjunction with the multiplexing hierarchy of DRAMA [13]. Encryption in the access area may take the form of end-to-end security, or an enclave encryption strategy, or both.

1. CURRENT STRATEGY

DCA plans currently have specified an end-to-end access encryption concept which calls for the implementation of digital secure voice terminals (DSVT) homed on a digital access area exchange (DAX) switch which will be unmanned and will contain no security equipments. It is anticipated that each secure subscriber will either have his own secure terminal or will be connected to the terminal by an extension device. Up to six extensions per DSVT will be possible.

The main issue to be considered is what other encryption strategies, in addition to the current strategy, could be applied to DCS subscribers in the access area. This issue is a function of type and number of subscribers and the environment in which they exist.

2. ENCLAVES

An enclave, as used in this report, is defined as a physically contained area, such as a building, in which a body of subscribers is located. An example of an enclave is the Defense Communication Engineering Center (DCEC) building. A secure enclave is an area to which some measure of physical, and possibly electronic security has been provided. The National Security Agency (NSA) headquarters is such an example.

DCS subscribers resident in enclaves that are secure, or capable of being secured, are candidates for enclave encryption. The encryption may include line concentrators, multiplexers, and secure private branch exchanges. The existence of enclaves, raises the possibility of obtaining authorization to pass classified information over local loops within the enclave. Secure communications between the enclave and the network would be established through an interface device defined as part of any encryption strategy.

3. SYSTEM ISSUES

There are four key system issues that affect the establishment of

communications security in the access area. These are: the environment in which secure subscribers exist, including any physical security; COMSEC techniques; timing and synchronization strategies; and the cost of securing the subscribers.

a. Environment. Environmental considerations include the location of subscribers desiring security, the level of physical security required, the potential for secure enclaves, and the possible interconnection of enclaves.

Subscriber location implies not only geographic location, but also location in relation to other subscribers. For example, the candidate backbone switches for overseas and CONUS deployment are markedly different. Overseas, the backbone switch will be RED/BLACK and will be capable of terminating approved (RED-analog) calls. Such calls would be transmitted on approved, physically secure, transmission lines. In CONUS, the switch will be BLACK, and will not terminate this type of call. All calls traversing such a switch will be either those not requiring security or those encrypted, on a call-by-call basis, in the access area.

The subscribers' location with respect to other subscribers impacts the alternatives that can be used to secure his calls. For example, a user who is isolated from a body of subscribers may require special provisions for call security, such as a DSVT or an approved line, versus a body of subscribers that may reside in an enclave and can be secured using an alternative designed for secure enclaves.

Physical security is an importar part of the environment. For example, both DCEC and NSA Headqua' s are secure enclaves. Each of these enclaves has different physical security requirements. At DCEC, there does not appear to be the need for fences and special guards as is the case of NSA. In addition, the Pentagon requires that transmission lines, terminating secure subscribers, and their associated main terminals be encased in intrusion resistant conduit for security purposes. This may not be necessary for secure enclaves such as DCEC. Overseas, secure enclaves may require special provisions such as fencing and periodic guard inspection. However, such provisions have not yet been determined for the CONUS or overseas.

The potential for secure enclaves exists in the DCS. For example, there are groups of subscribers on military bases who require call security and satisfy the enclave definition. The potential for setting up a secure enclave to provide the requisite security determines the applicability of the concept. This does not imply that failure of an enclave application obviates securing their calls. There are other schemes capable of providing needed call security, such as the current DCS strategy previously mentioned.

Military bases also provide an example where more than one enclave may exist in a local area. Therefore, there is the potential for interconnecting these enclaves to form a subnetwork within the DCS. Such an interconnection is envisioned for the current DCS strategy.

b. COMSEC Techniques. The COMSEC techniques to be used in the DCS encryption strategy will not be discussed in this report but are available in [14].

c. Timing and Synchronization. Synchronous digital terminals homed on an access area switch will require timing. This timing can be obtained from an access area switch (AAS) to which the terminal is homed. If the terminal operates in an asynchronous manner, it can generate its own timing. The AAS will also require timing for its operation. This timing can be derived from backbone switch connections in a master-slave arrangement or can be provided by its own internal clock, among others [15]. Access area synchronization is discussed in section VII.

d. Security Costs. As mentioned, the environment in which secure subscribers exist is a major system issue. This issue impacts the cost of providing the requisite access security in terms of the equipment needed and the level of physical security required. Cost implications are discussed in section V-6.

4. SUBSCRIBER REQUIREMENTS

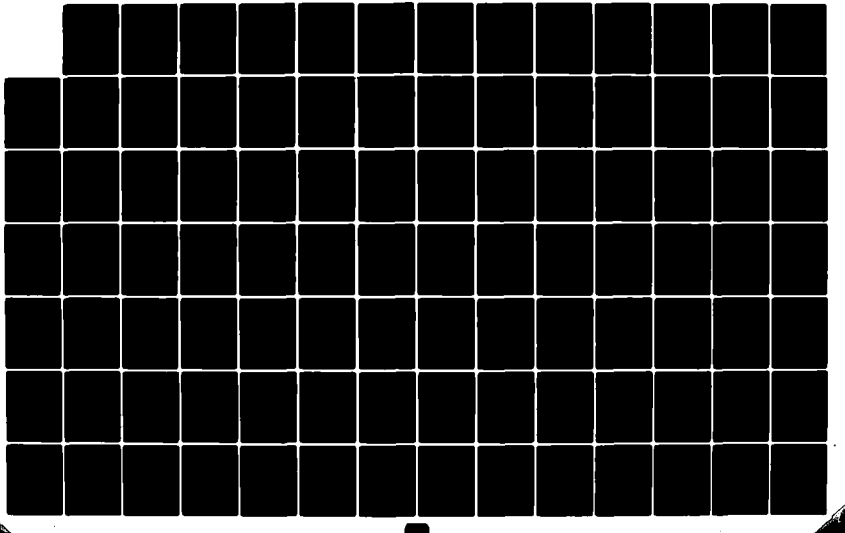
In response to a request by the Director, DCA, the JCS requested each MILDEP, Unified/Specified Command, and DoD Agency to prepare a list of proposed secure voice subscribers to be satisfied by the DCA Secure Voice program, AUTOSEVOCOM II. These lists were to be based solely on mission and operational security considerations. These listings are discussed in reference [16], and are also given here as background for subsequent discussion of alternatives for providing access area security.

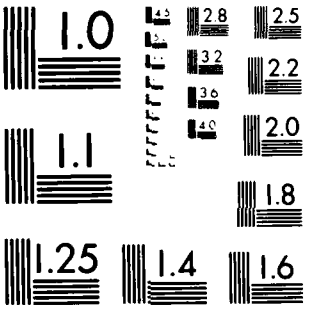
a. Distribution by Theater. Table 5-I shows the subscribers distributed by theater of operation. The entries reflect requirements for terminals, extensions, and protected wire extensions. The protected wire extensions range from 1 to over 4000. At the low end of this scale, requirements are interpreted as extensions from a secure voice terminal. At the medium and higher end, the requirements reflect a need for a RED type distribution system.

b. Distribution by Major Initiating Authority. The distribution of user requirements by major submitting authority is given in Table 5-II, from a breakout of the entries in Table 5-I. This table and other breakouts can be used to project the voice traffic demand represented by the approved subscriber list [16].

AD-A134 583 SYSTEM INTEGRATION AND INTERFACE TRANSITION ISSUES(U) 2/3
DEFENSE COMMUNICATIONS ENGINEERING CENTER RESTON VA
APR 77 DCEC-TR-2-77

UNCLASSIFIED F/G 17/2 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

TABLE 5-I. AUTOSEVOCOM II SUBSCRIBER DISTRIBUTION BY THEATER OF OPERATION

	Terminals	Extensions	Protected Wire Extensions	Totals
Europe	1233	818	446	2497
Pacific	918	380	61	1359
CONUS/Canada	4154	2043	4809	11006
Alaska	140	64	17	221
Caribbean	111	39	0	150
Other	38	11	0	49
TOTALS:	6549	3355	5333	15282

TABLE 5-II. AUTOSEVOCOM II SUBSCRIBER SUBMISSIONS BY MAJOR INITIATING AUTHORITY

Submitting Authority	Terminals	Extensions	Protected Wire Extensions	Totals
OASD/JCS	33	47	530	610
CINCPAC	820	483	54	1357
CINCEUR	1113	775	380	2268
CINCLANT/CINCLANTFLT	110	388	0	498
SAC	771	0	0	771
NORAD	349	107	58	514
ALASKAN COMMAND	62	26	0	88
SOUTHERN COMMAND	76	19	0	95
OTHER ARMY	361	57	17	435
OTHER NAVY/MARINE	622	234	115	971
OTHER AIR FORCE	1290	1064	0	2354
DCA	56	48	0	104
NSA	84	24	4065	4173
OTHER DoD AGENCIES	136	36	3	175
OTHER GOVERNMENT	707	3	111	821

c. Distribution by Functional Category. A requirements breakout by functional category is given in Table 5-III. It is important to note that the first three entries constitute the majority of the requirements independent of the theater of operation.

It cannot be determined from these tables alone which subscribers require secure terminals and which require only extensions off the terminal. Such a determination would require in-depth knowledge of the environment in which they exist. This environmental knowledge would also be necessary before any potential enclaves could be addressed.

5. CONSIDERED ENCRYPTION ALTERNATIVES

Alternatives for encryption in the access area cover a wide range; however, those considered here are but a subset of a much larger set that could be studied. Constraints imposed by present DCS programs for transmission and switching have been considered in the formulation of these alternatives. Specifically, the alternatives to be considered include: End-to-End security (alternative I); A/D conversion with concentration in the access area (alternative II); and PBX-to-PBX Security (alternative III). It can be seen that both alternatives II and III are concerned with enclave encryption, where the enclave may be nothing more than a secure room, and that alternative I is concerned with encryption at the subscriber's end instrument. Figures 5-1 through 5-3 conceptually show the alternatives. Mixes of both analog and digital subscribers are assumed where appropriate.

a. End-to-End Encryption

(1) Definition. This alternative presumes that signal encryption is provided down to the subscriber end instrument. Current DCS programs have specified a DSVT with up to six extensions for each instrument. This alternative is also characterized by a digital access switch. A DAX has been specified for this function. It will accept both secure and nonsecure digital traffic, and will be connected directly to a tech control and backbone switch. DAX's will have the capability of being interconnected. Because the DSVT will A/D convert and encrypt analog voice, the encryption being optional and obviated for nonsecure calls, there is no need for encryption on the transmission lines between the DAX and the backbone switch.

(2) Advantages. The major advantage of this alternative from a systems viewpoint is that encryption is provided end-to-end. Thus the originating encrypted stream will never need to be decrypted anywhere in the network. Only at the destination DSVT will decryption result. This alternative is independent of the environment in which secure subscribers exist, provided physical security for the DSVT is

TABLE 5-III. DISTRIBUTION OF AUTOSEVOCOM II SUBSCRIBER SUBMISSIONS BY FUNCTIONAL CATEGORY

Functional Category	Theater of Operation			Contgcy.	Total
	CONUS*	Europe	Pacific		
Command and Control	1907	516	337	12	2772
Intelligence	4871**	335	253	4	5463
Operational	2706	1015	514	33	4268
Logistics	638	322	100	0	1060
Diplomatic	5	18	7	0	30
Common User	876	44	111	0	1031
Other	374	79	37	0	490
Blank Entries	-	168	-	-	168

* Includes Alaska, Canada, Caribbean
** Includes 4000 NSA Grey Phone Extensions

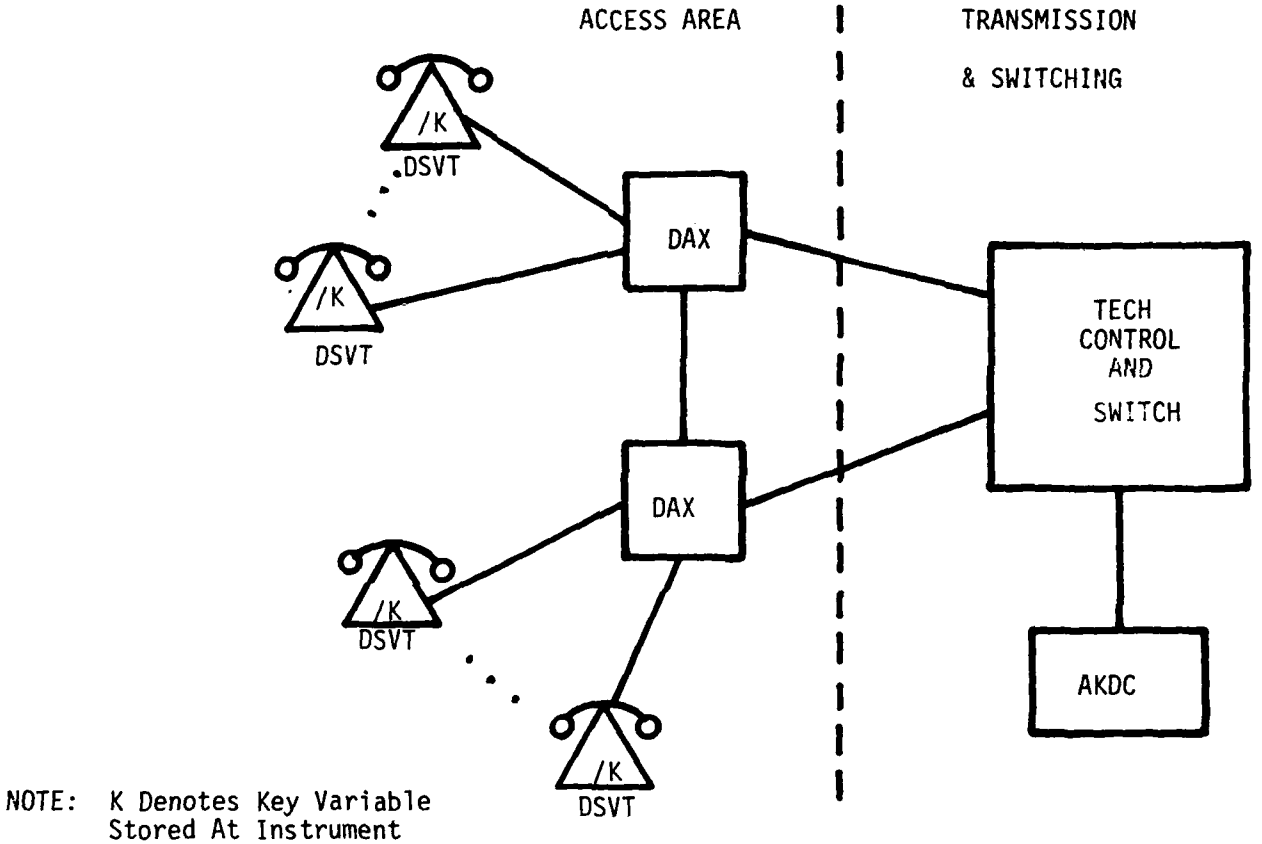
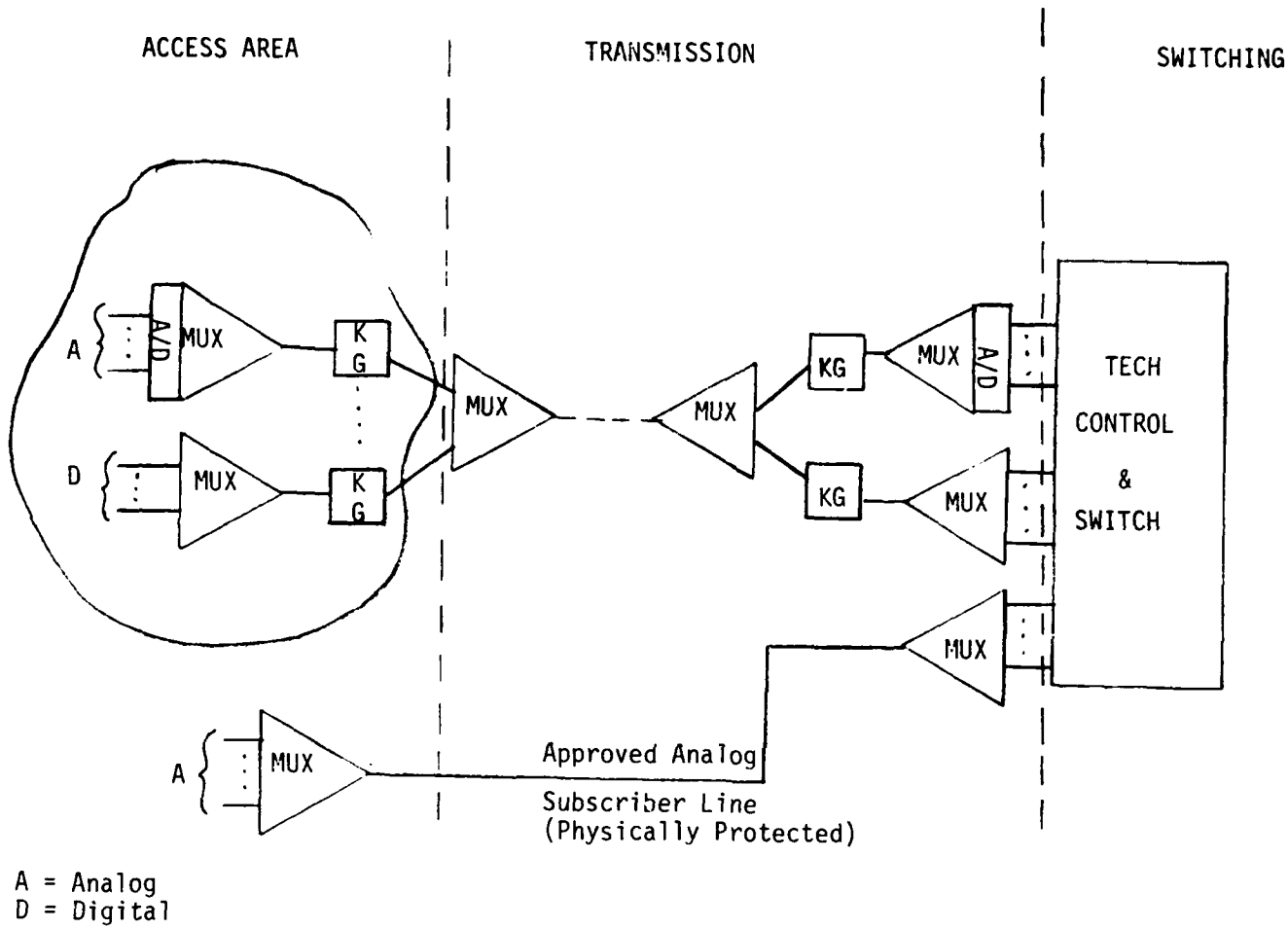


Figure 5-1. End-to-End Security (Alternative I)



A = Analog
D = Digital

Figure 5-2. Bulk Encryption (Alternative II)

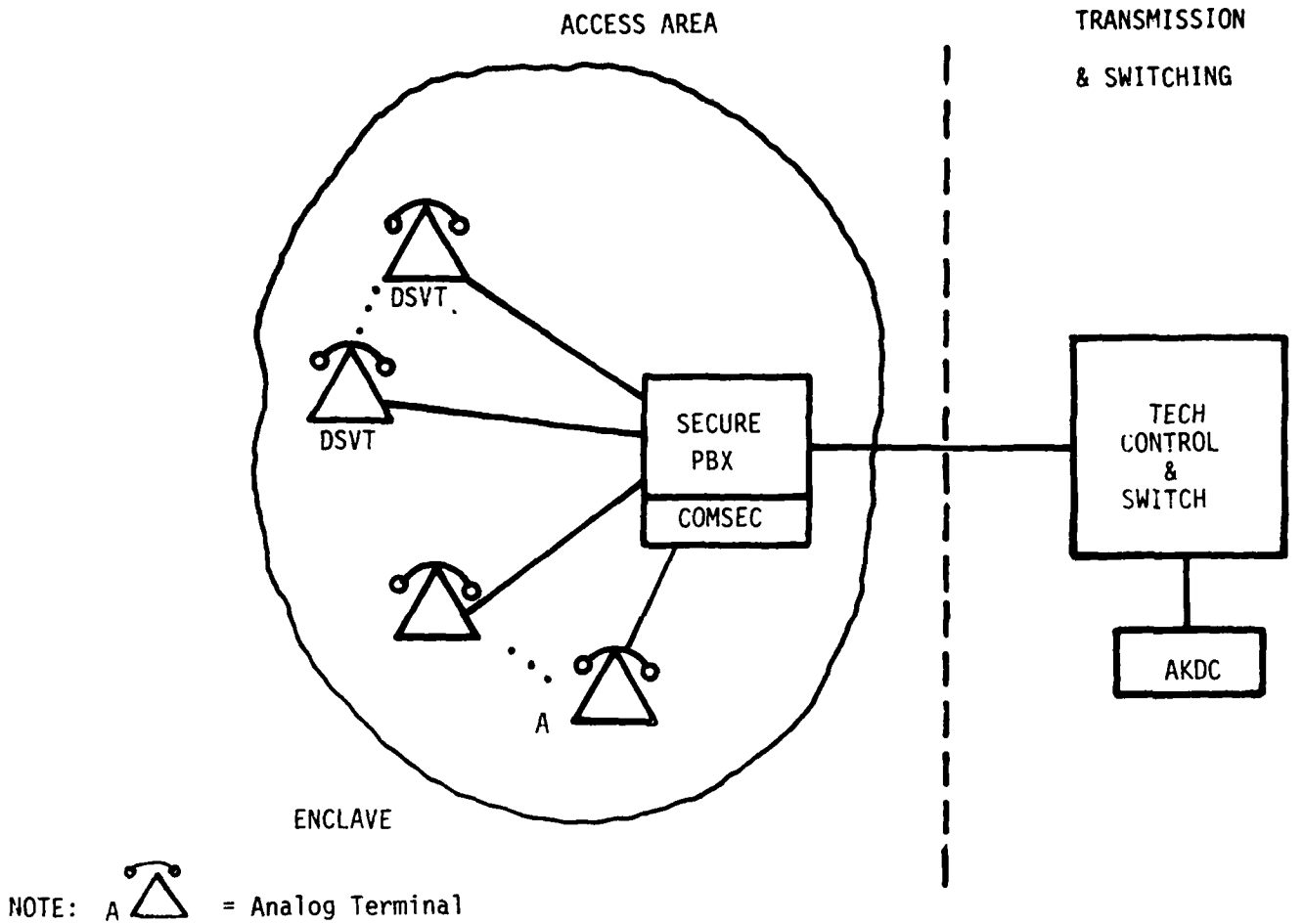


Figure 5-3. PBX-to-PBX Security (Alternative III)

available. This includes application to isolated subscribers and to enclaves whether secure or nonsecure. That a DSVT can have as many as six extensions is key factor because the subscriber population will not require one DSVT per subscriber. Rather, several subscribers can share a DSVT, thereby reducing initial investment and operation and maintenance costs. This will result in a smaller number of terminations required of the DAX, further reducing costs as compared to a DSVT per subscriber.

(3) Disadvantages. The alternative is characterized by one major system disadvantage. It does not allow for the DAX to accept any subscriber transmission signals that are not DSVT derived. This precludes the use of the DAX for any purpose other than processing DSVT originated or terminated traffic. It will be possible to interconnect DAX's, but only DSVT derived traffic will be carried among them.

b. Bulk Encryption

(1) Definition. This alternative, as depicted in Figure 5-2, is characterized by encryption of a given number of subscribers, either digital or analog in format Analog subscribers would be converted to a digital equivalent and concentrated before being encrypted. Digital subscribers would be concentrated before encryption. The digital stream would be bulk encrypted in the enclave before entering the transmission subsystem at some nominal rate. At the switch side of the transmission subsystem, the streams would be decrypted and demultiplexed to baseband. These resulting digital streams would be directly input to the switch if they are bit rate compatible with the switch. If they are not, a code conversion algorithm would be required to establish the compatibility.

Figure 5-2 also shows an approved analog access line that is physically secured, rather than electronically secured. Inputs to the multiplex would be analog and would remain analog. At the backbone switch end of the transmission subsystem, the transmitted stream would be multiplexed and input directly to the analog part of the backbone switch, presuming that the switch is capable of accepting analog inputs. The technical control facility associated with the AN/TTC-39 switch will have provisions for approved access lines. However, at present there are no known DCS requirements to terminate RED analog calls at AN/TTC-39 switches [16].

(2) Advantages. This alternative is independent of traffic type and mix, which is not true of alternative I. Concentration can be employed such that entry into the transmission can be made through a multiplexer as shown in alternatives I and II of the digitization strategy (section IV). This alternative does not require an access

switch for its operation. Also, if subscribers were located close to the switch, they would be brought into the network on an approved access line.

(3) Disadvantages. This alternative has several major system implications. For traffic distribution at the backbone switch, the bulk encrypted lines must be decrypted and demultiplexed. This would add a new dimension to the transmission multiplex hierarchy planned for the transitional period. Presently, there are no DCS transmission programs to decrypt/demultiplex bulk encrypted access lines. If the bulk encrypted access lines were input to the transmission subsystem, say at the 1.544 Mb/s rate of the DRAMA hierarchy, there would be the problem of encryption imbedding that is related to dynamic communications stability, which will be discussed in section VII. Also, the decrypted, demultiplexed streams would enter the backbone switch in the clear (RED calls). This would also be true for every switch in the path that the call must traverse on the way to its destination. These RED calls would be encrypted between switches. While this is not a major disadvantage for overseas deployment, compared to alternative I, it would be impossible for CONUS switches, which will be BLACK and not capable of processing RED analog calls. Hence, this alternative is obviated for application in CONUS access areas. The only possible exception to this would be cases where the bulk encrypted lines are destined for a single location and hence, do not require switching or adding and dropping of individual subscribers. Finally, as noted previously, if the bulk encrypted streams are not bit rate compatible with the backbone switch to which they are homed, a code conversion must result. For example, if a CY-104 were used as the A/D multiplexer-encryption device to provide bulk encryption, each subscriber would be A/D converted to 64 kb/s. This rate, however, is not compatible with the basic rate structures acceptable to the AN/TTC-39 switch. This would entail a code conversion from PCM to a 16 or 32 kb/s code without going through any D/A-A/D conversion pair. Only then could the individual streams be switched.

c. PBX-to-PBX Encryption

(1) Definition. This security concept is characterized by a RED/BLACK access switch which provides both A/D conversion and encryption functions. As discussed in reference [17], it is a technically feasible approach to securing certain subscribers, but one which appears to have application only in secure enclaves.

The concept, as depicted by Figure 5-3 in an enclave environment, allows for both analog and digital traffic to be input to the switch. Analog traffic would be A/D converted at the switch. Those subscribers requiring security would have their communications secured at the switch, the encryption equipments being resident and pooled at the switch. Subscriber access lines between terminals and the switch would be

analog, except where digital terminals exist such as DSVT's and data terminals. In essence, this alternative emulates alternative I, except that COMSEC has been transferred from the subscriber terminal to the secure PBX.

This concept allows for intra area and interarea communications, the interarea being divided into the backbone area and other access areas. In this concept, the action taken by the PBX on subscriber calls as a function of destination is given in Table 5-IV.

(2) Advantages. In this alternative, the secure PBX will accept both analog and digital traffic, where the digital traffic may be originated, for example, by DSVT's. As in alternative I, encryption would be on a call-by-call basis. Therefore, no decryption would be needed anywhere in the network except at the destination subscriber's PBX or terminal. This alternative would allow communication between a homed subscriber and distant DSVT's by using DSVT-type COMSEC equipments, thereby facilitating interoperation with alternative I. COMSEC equipments would be pooled at the secure PBX and allocated on as-needed basis. This would reduce COMSEC costs compared with alternative I, which deploys a predetermined number of secure terminals.

(3) Disadvantages. Application of this alternative is environment-dependent, and is limited to secure enclaves. Hence, both physical security, and operation and maintenance considerations are impacted. Physical security for this alternative depends explicitly on such factors as requirements to secure the analog access lines between the subscriber terminal and the secure PBX, periodic surveillance of these lines, and external enclave protection including fencing and manpower. If the secure PBX requires manning, operation and maintenance factors will seriously escalate the cost for this alternative. However, these depend on the level of security provided the enclave, and whether the COMSEC equipments can themselves be adequately secured within the enclave confines. Communications are not end-to-end secured but rather PBX-to-PBX, or PBX-to-called subscriber secured. Secure communications are therefore in the clear between the subscriber analog terminal and the secure PBX. This is a disadvantage when compared to alternative I.

6. COST CONSIDERATIONS

The costs associated with the three alternatives include equipment, O and M, and physical security. The equipment costs are those for secure terminals, A/D and crypto devices, access switches, backbone access lines and protected wire distribution.

a. Assumptions. Certain basic assumptions have been made for the costing analyses of the alternatives. These are needed because of incomplete knowledge of the existing communications environment.

5- IV. PBX ACTION ON SUBSCRIBER CALLS

Subscriber Traffic	Destination	PBX Action
Non-Secure	Intra area	Analog I/O, no A/D
	Intra area	Analog input, A/D, No COMSEC
Secure	Intra area	Analog I/O, no A/D, No COMSEC
	Intra area	Analog input, A/D, pooled COMSEC, KDC key acquisition, key storage

Specifically, in the initial cost comparison of alternatives I and II, physical security requirements have been assumed to be the same. However, a parametric analysis is subsequently given to show the factor increase in the security cost of alternative III as compared to alternative I, since it is very likely that physical security costs will be greater for alternative III. These costs must be considered on an implementation case-by-case basis. Access line costs between the access switch and associated backbone switch have not been considered.

Equipment cost factors are based on DCEC cost estimates and are discussed in detail in reference [18], with the exception of Alternative II equipments. For alternative II, it is assumed that an existing CY-104 having 24 individual A/D, multiplexing and encryption capabilities, can satisfy bulk encryption needs. It is further assumed that redundancy is required and that a similar device will exist at the backbone switch due to the lack of code converters and because provision has not been made for terminating these subscribers in present DCS programs.

Because there are no known DCS requirements for approved subscriber lines and because transitional DCS CONUS switches have no provision for approved lines, this part of alternative II was not costed.

Table 5-V shows the equipment specifics and the O and M factors. Physical security costs have not been considered.

Since the costs associated with alternative III are based on pooled equipments, a statistical characterization is used. For the analyses it is assumed that subscribers originate .2 calls per busy hour with a holding of 5 minutes, and a 1% switch blocking probability.

b. Cost Tradeoffs. Figure 5-4 shows the results of the costing analysis where it has been assumed that the secure PBX, for alternative III, is unmanned. Encryption requirements are assumed to have been physically secured within the switch which is imbedded within the enclave. The curves in Figure 5-4 are a function of the number of DSVT extensions for alternative I, and the number of analog phones attached to the same address number for alternative III.

Costs for bulk encryption are constant over the full range of subscribers. This results wholly from the traffic and blocking statistics which indicate that one secure terminal can service up to 145 subscribers with one channel being held as a spare.

TABLE 5-V. COST CONSIDERATIONS

ALTERNATIVE	TERMINAL (T)	SWITCH (S)	O&M	PHYSICAL SECURITY (PS)
End-to-end (I)	DSVT	DAX	% of T+S	See note 1 & Table 5-1
Bulk (II)	CY-104		% of T	See note 1 & Table 5-1
Secure PBX (III)	Analog	Secure PBX	% of S	See note 2

Notes:

1. 2 men, 3 shifts at $10K/man/year
2. % of PS for Alt I (and II)

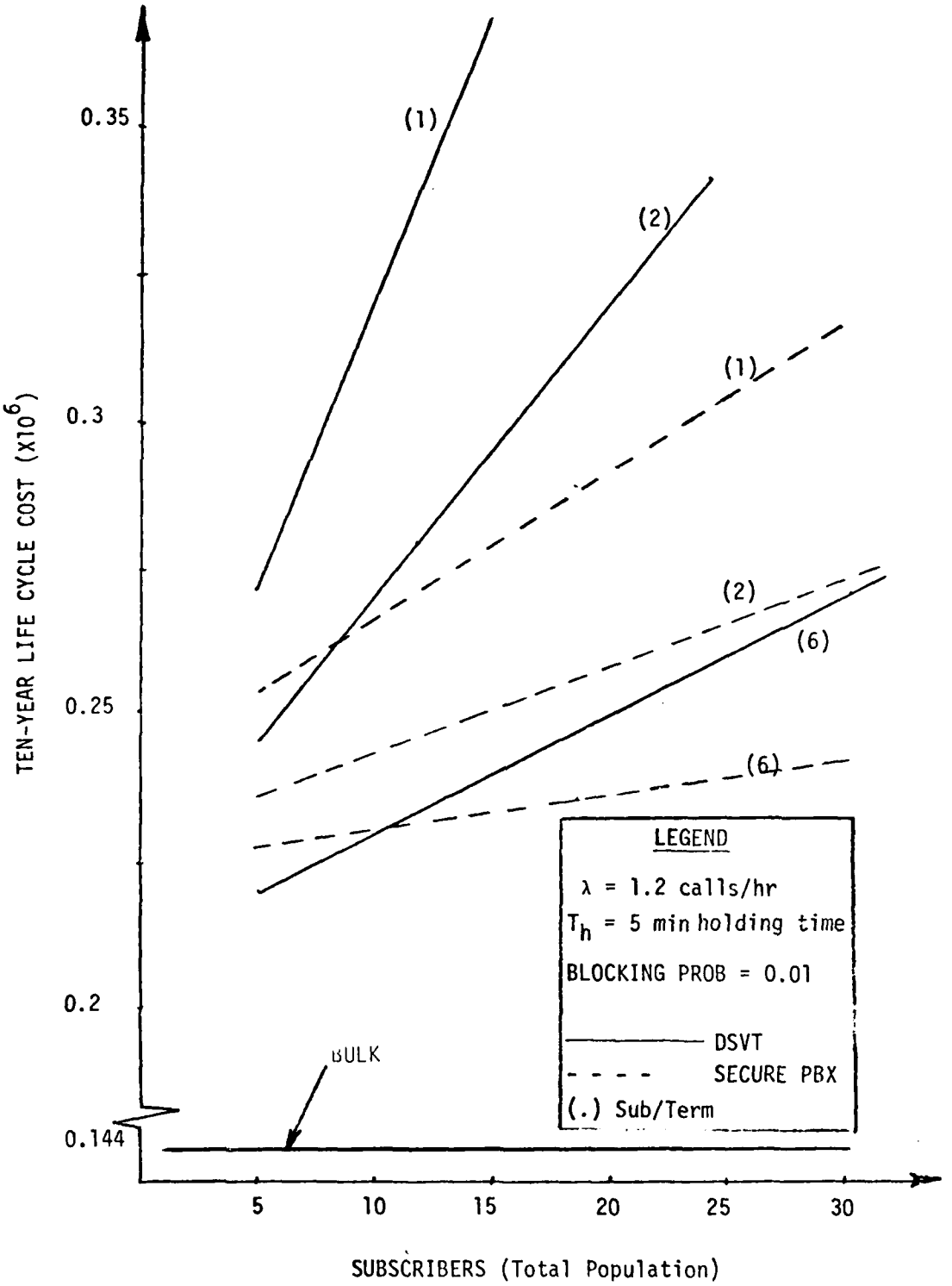


Figure 5-4. Ten-Year Life Cycle Cost Versus Subscribers-Unmanned PBX

It can be inferred from Figure 5-4 that there are subscriber regions in which one alternative dominates others. It is apparent that bulk encryption has significant advantages over DSVT or secure PBX concepts for the full range of subscribers. However, as previously mentioned, there are operational difficulties with bulk encryption in securing the information in the backbone area.

c. Operation and Maintenance. Of the cost factors involved, O and M produces a significant change in the life cycle costs. For example, if all assumptions remain unchanged except the manning assumption for alternative III, significant differences in the application of the alternatives to specific subscriber population will result. Figure 5-5 shows this manning change cost effect to alternative III. With two extensions chosen as an illustrative example, the results of this figure indicate that for less than approximately 54 subscribers, the DSVT concept is preferred over the secure PBX concept. For alternatives I and II, O and M is assumed unchanged. The cost increase is significant when compared to the previous unmanned case in which the secure PBX alternative was always preferred for two extensions.

d. Physical Security. The cost associated with physical security is also significant. For the previous analyses presented it was assumed that physical security for both alternatives I and II was identical. However, for alternative III, physical security may be required depending upon the environment, because the analog subscriber lines may need physical protection or because security external to the access area might be necessary. The associated costs for the alternatives would be greatly affected.

As an example, consider 2 subscribers on the average per terminal, and a population of 20 subscribers. From Figures 5-4 and 5-5, the cost for alternative I is D = \$322K; for alternative III, the costs are E_o = \$257K for the unmanned case, and E_o = \$452K for the manned case. These values are used as a base for Figure 5-6 which shows the effects of increasing the physical security cost of alternative III above that of alternative I. The initial cost for physical security common to both is indicated on the figure. Alternative III costs are found by multiplying the ordinate factor, N, by the sum of D_o and the initial physical security cost.

7. DISCUSSION

Of the key issues discussed, the environment appears to have the most serious impact on the application of the alternatives to securing DCS subscribers. As noted, alternative I is environment independent, whereas alternative III depends explicitly on the environment, mainly as a function of physical security. DCA has no stated requirements for alternative II; hence, it is not considered a likely candidate for inclusion in the DCS.

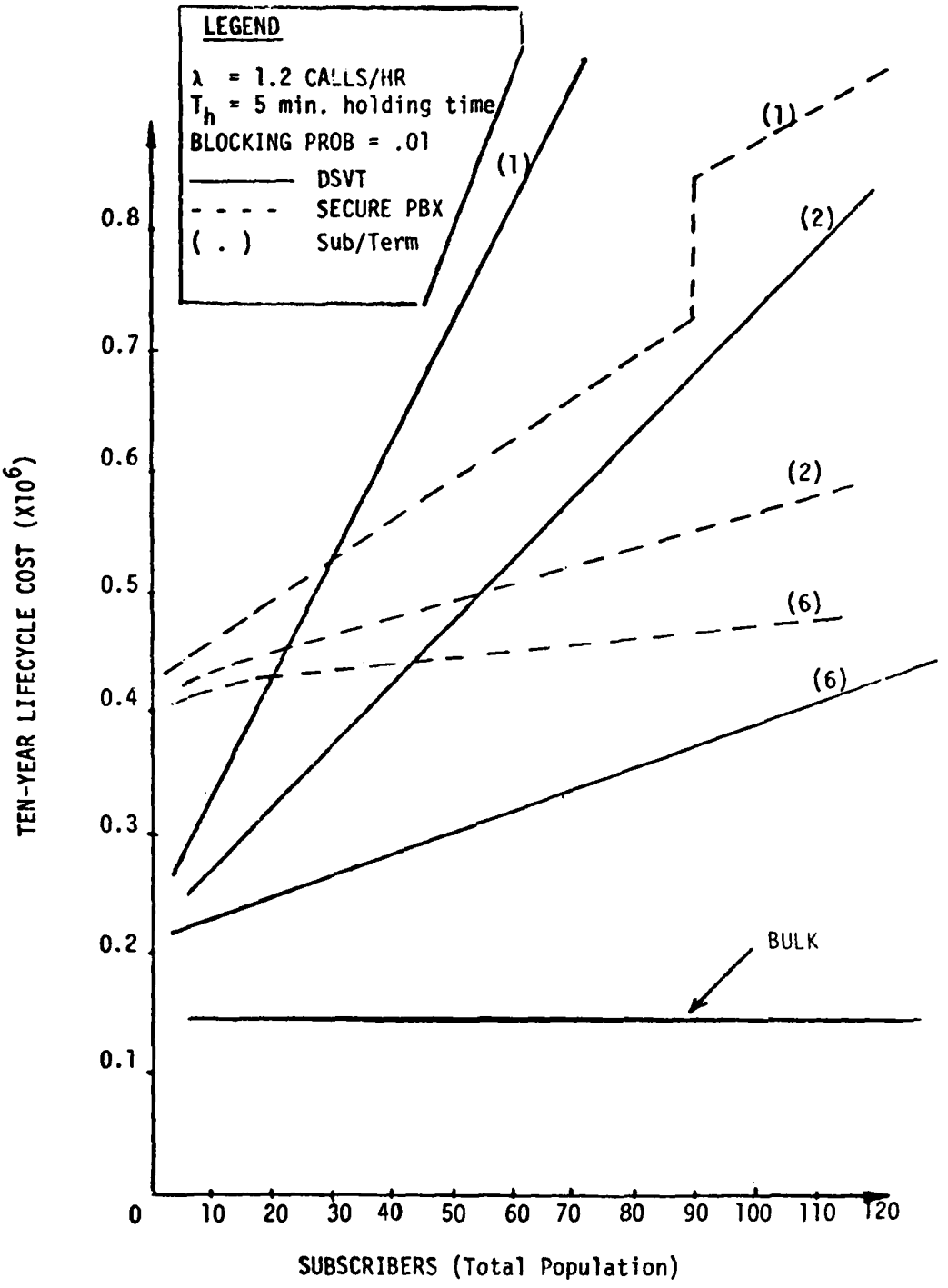


Figure 5-5. Ten-Year Life Cycle Costs Versus Subscriber-Manned Secure PBX

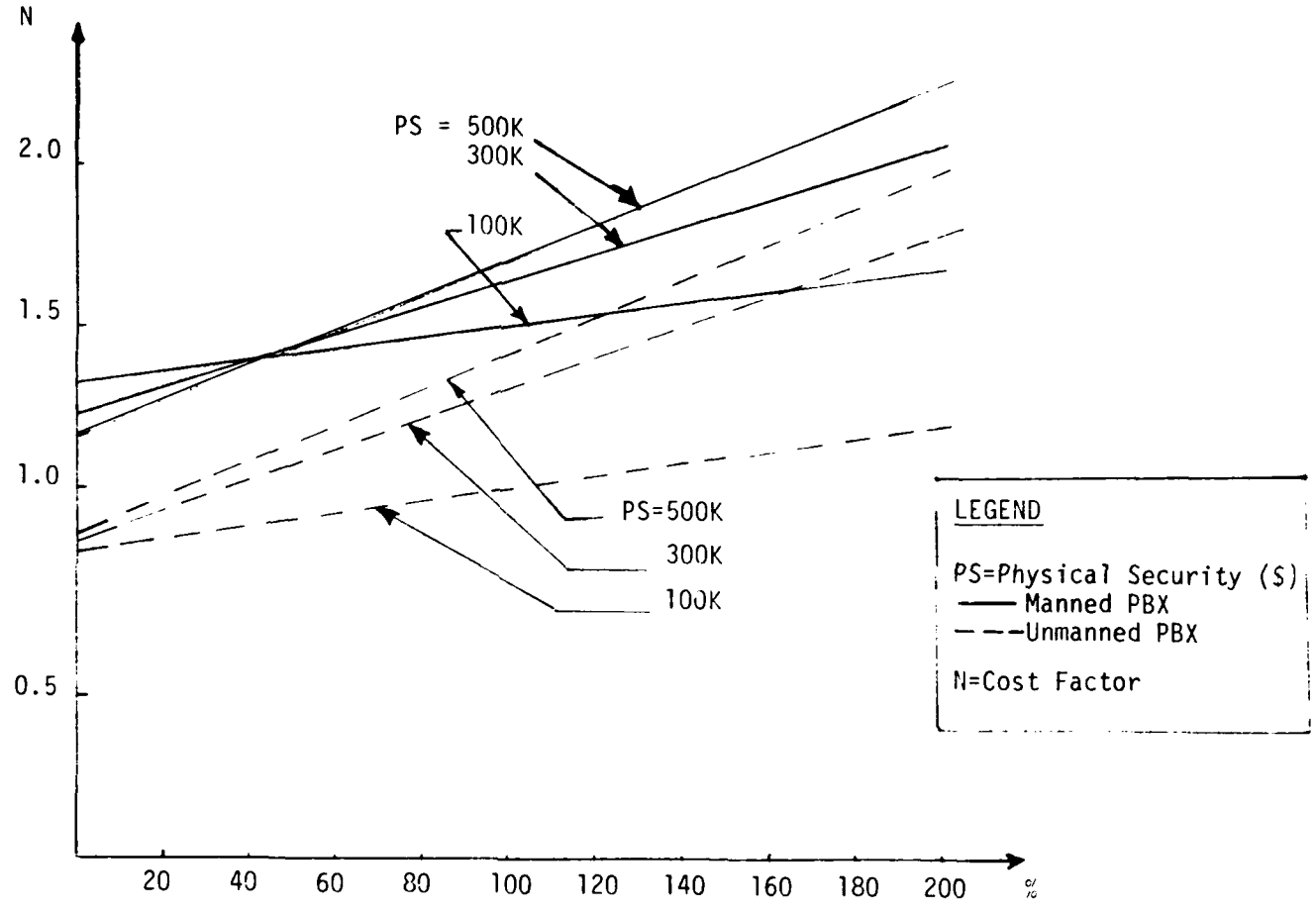


Figure 5-6. Increased Physical Security Costs (Ten-Year Cost) For Alternative III

The data submitted in Tables 5-I through 5-III support the conclusion that both alternatives I and III can find DCS application, but present programs do not include any provision for interoperation.

The cost analysis, though specific as far as assumed statistics are concerned, has shown that there are subscribers populations for which alternative I is preferred over alternative III, and conversely. It further demonstrates that there is potential application for both alternatives.

VI. SOFTWARE COST MINIMIZATION

1. THE TREND OF SOFTWARE COST

In recent years the increased use of computers within the Defense Communications System has caused a software cost explosion. While state-of-the-art advances in technology have kept hardware cost down, costs in the labor intensive area of software are rapidly rising to the point where it is becoming the dominant contributor to computer system cost. For example, software cost within DoD has been reported in excess of $3 billion per year [19]. For the Air Force, the current software/hardware ratio of total automatic data processing system cost is greater than 65/35, and based on current estimates the ratio will swell to 90/10 by 1985 [19]. The increased dependence of the DCS on computing capability and the continued increase in the ratio of software to hardware cost emphasize the need for additional effort in the area of software cost minimization.

The utilization of software is expected to increase in the next decade. For example, three related areas of development that presently require software support are: computer security mechanisms, computer networking, and distributed systems built from microprocessors. In order to harness and consolidate the potential of many microprocessors or computers for a particular effort such as computer networking, their activities must be coordinated and controlled by software [20]. If such a processing environment is expected to handle classified as well as unclassified data, then additional precautions must be taken to ensure that the software performs specific functions, and under no conditions does it perform unexpectedly.

The intent of this section, is to examine why the development cost of software has continued to increase relative to hardware, identify opportunities for a reduction in the cost of software production and maintenance, and recommend the action necessary to improve the quality and reduce the cost of software. Furthermore, significant changes in requirements being placed on software are identified, and some trends occurring in software development in the future are outlined. It is hoped that this section may serve as a catalyst for realistic and fruitful action.

a. Factors Influencing Software Cost Estimation. The following are factors to be considered in estimating cost:

- Number of Source Instructions. This is a measure of the complexity of the task. A major problem in large systems is

the increase in cost per instruction as the number of instructions increases. For example, one study [21] reported that the development rate for instructions per hour ranged from .33 to .53 for large real-time programs (programs over 100,000 lines of code), to 1.6 to 5 instructions per hour for programs from 5,000 to 20,000 instructions, under similar conditions.

- Source Language Programming. The time required to develop a program using assembly language has been reported as high as twice the time required if a high order language is used [22]. A more recent study [21] involving the development of real-time systems indicated a 20% reduction in total development effort through the use of a higher order language. Software costs for a given number of statements tend to be similar whether the program is written in a high order language or assembly language. Thus, the saving is a direct result of fewer statements being written with a high order language. High order language programming also tends to result in better programming algorithms and easier program maintenance, since the programmer, by having to look at fewer instructions, is able to group a large portion of the problem and/or understands the problem more rapidly.

- Type of Application. The cost for real-time applications has been estimated as much as five times greater than for non-real-time applications [22]. The communications systems development would be considered a real-time application. Personnel from Bolt Beranek and Newman, Inc., during a meeting held at the Defense Communications Engineering Center in October 1976, estimated that executive system software cost is approximately three times the cost of compiler language software on a per-instruction basis. Furthermore, it was predicted that communications software costs are approximately three times greater than executive system software costs. Another study [21] indicated that large real-time programs required four to five times the development effort necessary for support programs such as loaders, editors, assemblers, and utility programs. There is adequate information available to indicate a significant difference in the effort necessary for different types of applications.

- Participant's Experience. A recent study [21] concluded that the most important single factor which determined the different development rates was the experience level of the designing programmers and supervisors. In fact, development times may be reduced significantly if the program is a variant of a familiar program.

- Availability of Generalized Support Packages. An application which can utilize a support package such as a generalized management information system can accrue significant cost reduction; support package utilization should be evaluated and encouraged in appropriate circumstances. In fact, the availability of software support tools has been recommended [23] as a major consideration in the selection of a vendor for software development. Unfortunately, many support tools are both language and machine dependent.

- Size and Structure of the Data Base. Software that retrieves and utilizes information from external resources such as data bases costs more per instruction than similar programs without data interactions [22]. The processing requirements of data must be considered in the design phase so that proper checks and controls are implemented to avoid unnecessary termination of processing due to invalid entries.

- Turnaround Time. Interacting computing facilities can reduce turnaround. Current estimates [24] indicate at least a 20% improvement in program development by using interactive computing instead of batch processing.

- Hardware Constraints. Hardware procurement frequently precedes software development. If the hardware is improperly sized for the job or if the size of the job expands, attempts are frequently made to have the software compensate for hardware inadequacy. The availability of different hardware configurations through computer networking should enable the user to make better procurement decisions by allowing software development and sizing on a host computer prior to procurement of hardware. The actual delivery date of hardware may be less crucial, since considerable development and testing may occur within the network environment.

- Software Production Schedules. An unrealistically foreshortened software production schedule normally results in significantly higher project cost, provided the original schedule was well planned and realistic [21]. The quality of the product suffers; hence, the maintenance costs are increased. Management must consider these penalties when they shorten software production schedules. Current studies reveal that increasing the staff on a software project after it has been initiated frequently extends the length of the project instead of shortening it. Generally, the fewer the number of programmers, the greater the productivity per programmer.

- Expected Quality and Reliability. The functional capabilities expected from a specific software module dictate the expected quality and reliability. For example, software support for systems which simultaneously process different levels of classified material must be certified. The intent of certification is to ensure that the software performs as intended and does nothing more. Based on the current trend, it is anticipated that eventually this certification will require that the code is proven correct. Regardless of the approach, the cost of such software will include additional expenditures to ensure that precautionary measures have been taken to avoid security compromises.

- Development Environment. The development and testing of software may occur in an environment substantially different from the planned implementation environment. Some companies [21] have improved the production rate from 25 instructions per hour to 40 instructions per hour through the use of a simulator. In communications systems, simulation is difficult because of the real-time operating environment. Thus, the simulation must in many cases consider the relative execution time of routines.

- Stability of Requirements. Studies have shown that more development effort is spent in the 10 years following implementation than during the initial development [21]. Changing requirements will increase the life cycle cost of software; however, proper initial planning and analysis are essential to anticipate such changes and implement them in a timely and inexpensive manner.

- Personnel. Probably no field has a greater variance in the ability of personnel than software development; studies have shown ratios of productivity as great as 26 to 1 [24]. Furthermore, the more productive people tend to produce the more realiable software. Emphasis should be placed on proper selection and retention of quality people. Personnel are the most important ingredient in determining the success or failure of a system [21].

- Development Techniques. Techniques such as structured programming, automated aids, and chief programmers teams have contributed to a reduction in software cost [25, 21]. Appropriate research should be continued to develop, identify, and provide proven methods for future software projects.

- Management Involvement. Management must have a high degree of awareness and understanding of software so that they can initiate changes needed to lower the life cycle cost of software.

Management has the responsibility and the opportunity to make a significant impact on the software cost.

These factors are frequently used in the estimation of software costs. It is impossible to plan effectively and develop realistic costs if one cannot estimate expenditures for software. Although many companies [21, 22, 26] have developed methods to estimate software cost, these methods tend to be proprietary. The Government's problem in cost estimation is increased by the lack of available metrics. In regards to software, the term metric is defined as the standard which is a measure of the extent to which a module of software, or a system containing software, possesses and exhibits a certain property [27]. It is important to develop metrics that can be utilized by many different organizations. For example, a cost model may require specific inputs that describe the characteristics of the software, and if organizations intending to utilize these models do not have the proper data in the expected units of measure, then the results will be meaningless.

There is a need for additional research and/or investigation into the development of appropriate metrics and cost models. The Department of Defense does not possess the capability to evaluate different alternatives that require an accurate estimation of software cost. This deficiency is not caused by the lack of technological knowledge; rather it has occurred because there is a need to develop appropriate cost models and collect the supporting data.

b. Life Cycle Cost. Software costs are not as easy to identify and isolate as hardware costs. A hardware component has a fixed initial cost and some expected maintenance cost. The term "design-to-cost" is defined as the process utilizing unit cost goals as thresholds for managers and as design parameters for engineers. This concept has been reduced to practice for computing hardware; it is not fully understood for software.

The initial financial commitments for software are small compared to total commitment (see Figure 6-1). Software costs include all the effort involved in producing and maintaining the necessary executive, support, and application programs and their documentation; well defined functional specifications should also be included. Software development and maintenance can be represented by the following steps:

- Establish Performance and Design Requirements
- Develop Implementation Concept and Test Plan
- Develop Interface and Data Requirements Specifications
- Create Detail Design Specifications
- Complete Coding and Debugging

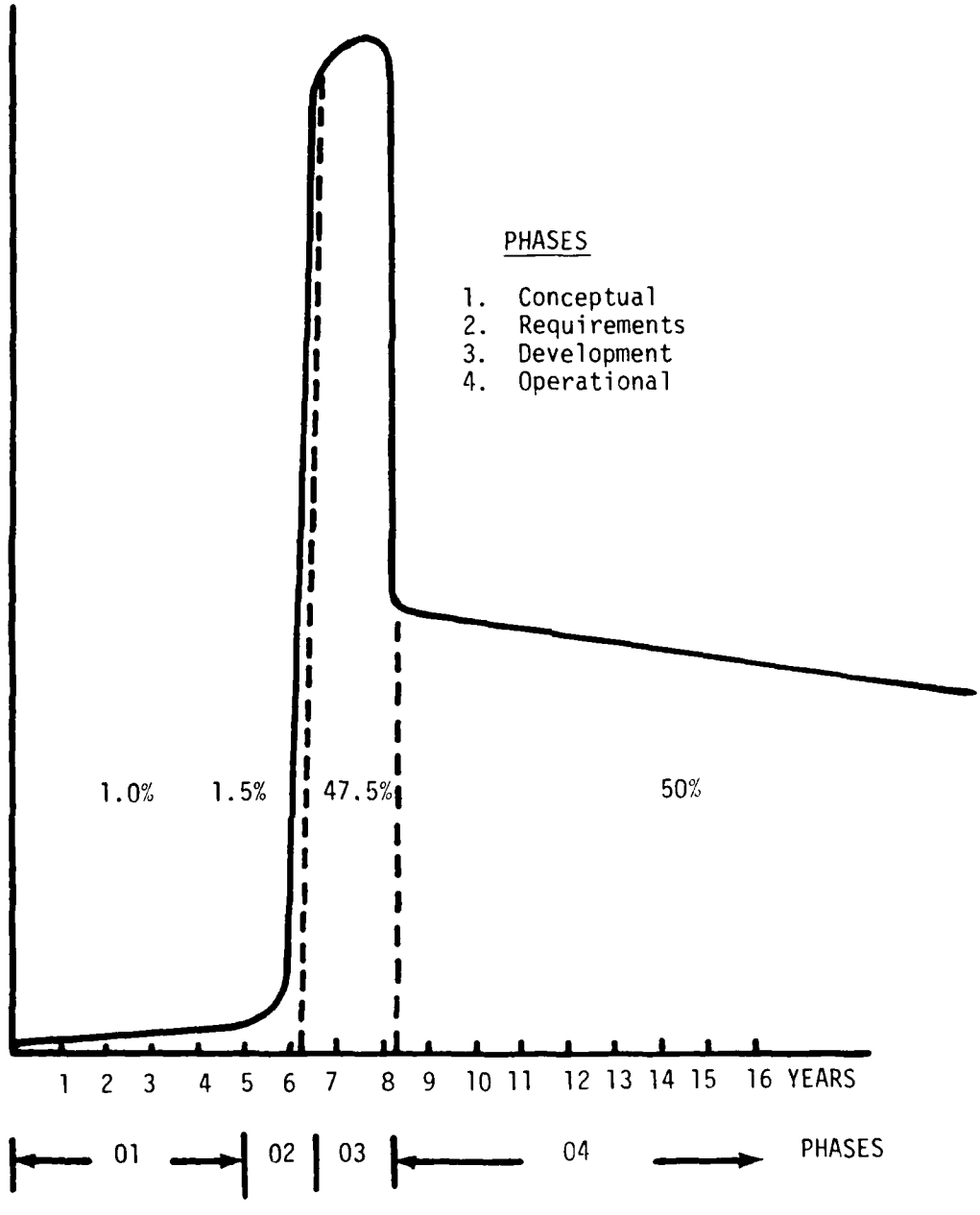


Figure 6-1. Composite Software Life Cycle

- Develop Software Documentation
- Complete System Validation Testing
- Document Certification and Acceptance Procedures
- Install and Check Out Operational Configuration
- Maintain and Update Existing Software

One should be aware that statistics currently available on the cost of different phases of the life cycle; these figures may be badly distorted [28] in that some of the largest systems are still in the process of development. Furthermore, maintenance cost will increase each year the system is in existence; some experts [21] have estimated that a system which required 46% of the life cycle cost for maintenance after 4 years may be expected to approach 60% of the life cycle cost in 10 years. A summary of the distribution of the development cost of several systems is shown in Table 6-I [19].

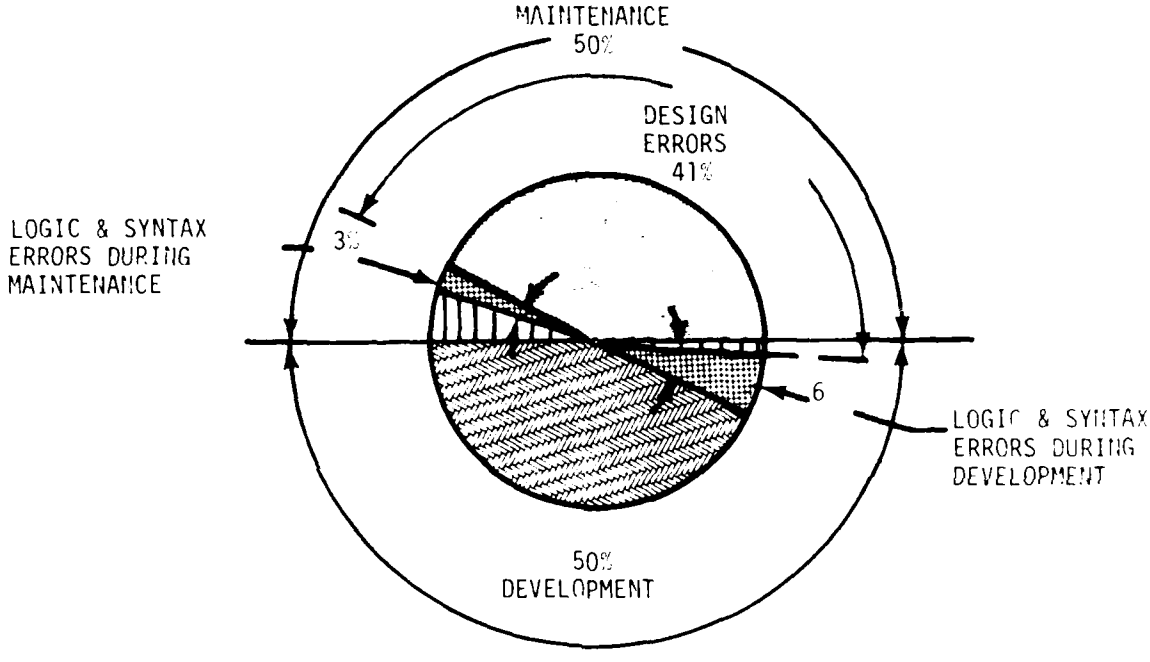
The interaction between different phases of the life cycle makes it difficult to assess the impact that one can expect from improving the performance and/or quality of the effort within a particular phase. For example, errors made during the design phase may not be identified until the maintenance phase; thus, their impact on cost would be reflected in the cost of maintenance (see Figure 6-2). Since the design and maintenance phases represent 65% of the total cost (based on today's statistics) and are attributed with more than 80% of the cost caused by errors [25], they should be the primary targets for improvement. Available data on cost of detection and correction indicates that design errors cost the most to diagnose and fix [21, 25]. The cost of detecting and resolving a software error after it has been placed into service is thirty times larger than the cost required to deduce and resolve an error during initial reading and review of code [21]. It has been reported that 70% of design errors are not identified until after development is completed. Obviously, it is very important to be aware of the impact that one phase can have on another phase. In the future one can expect an additional phase or function, proof of correctness [29], to be added to the life cycle of software where the software must be exceedingly reliable. Although it may actually be hidden in the coding and debugging phase, it should change the distribution of cost during the life cycle of the software. Furthermore, there are many functions such as documentation that affect the cost of maintenance; it is important that these related factors be evaluated in terms of total life cycle cost and not just their impact on the cost associated with a particular phase.

2. OPPORTUNITIES FOR REDUCTION IN SOFTWARE COST

Because of the interaction between phases of the life cycle, it is not clearly evident [21, 25] from the available analysis where the greatest opportunities exist for reducing cost. Furthermore,

TABLE 6-I. BREAKDOWN OF DEVELOPMENT COST FOR SELECTED SYSTEMS.

SYSTEM	ANALYSIS & DESIGN	CODING & DEBUGGING	VALIDATION
SAGE	39%	14%	47%
NTDS	30	20	50
GEMINI	36	17	47
SATURN V	32	24	44
OS/360	33	17	50
AVERAGE	34%	18%	48%



NOTE: The cost required to detect and resolve a design error after it has been placed in service is approximately thirty times larger than cost required to detect and resolve such a bug during the initial development.

Figure 6-2. Life Cycle Cost Attributed to Different Types of Errors in Development and Maintenance.

statistics currently available on the cost of different phases of the life cycle of software are somewhat deceptive [28]. These figures are badly distorted in that some of the largest systems are still under development, whereas those in maintenance were those produced in much less ambitious times. In most recent systems, one can expect the operations and maintenance cost to exceed those for development and acquisition by several times (see Figure 6-3) [28]. It does appear that design and maintenance are certainly two phases where an improvement could produce substantial savings (see Table 6-II).

Design and maintenance costs cannot be studied by themselves because there is an interdependency between all of the phases of life cycle software cost. For example, the utilization of a higher order language to promote transportability of valid code may have a significant impact on maintenance cost. Since software is expensive to develop and the same capabilities are developed for many systems (some are identical systems) it would appear logical to maximize the repeated useability of software. The ability to achieve this objective has failed to materialize because software historically has been structured to the architecture of the particular target computer. However, the continued increase in the cost of computer software, the introduction of transportability of software over a network, and a better understanding of software architecture as opposed to computer architecture enhances the likelihood of success.

Regardless of technical expertise, the ultimate responsibility for the high cost of software resides with management. Management has too long been in awe of the "Computer Revolution." It must take the necessary action to control software projects. The first step is to become educated in the principles of software so that software development and maintenance can receive the equivalent control and scrutiny given hardware [21, 23].

a. Software Design. The activities that are actually considered part of the design process vary depending on the reference [2]]. Frequently recognized achievements in the design process are the following [21, 25]:

- An overall functional specification describing what is to be performed.
- The dependencies between each major function and the modules which are expected to provide the functional support.
- The linkages between modules.
- A "structured" logic flow such as a system flow chart.
- All data structures and their corresponding intended usage, attributes, access method, and value range.

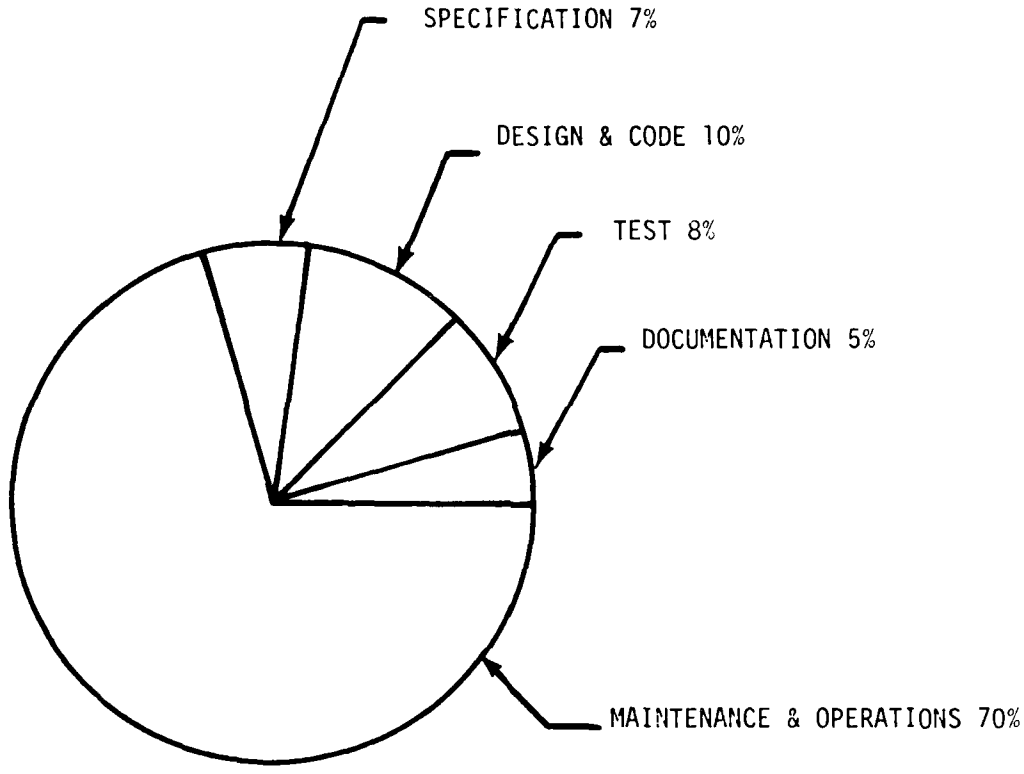


Figure 6-3. Estimated Distribution of Life Cycle Cost for Systems Currently in Development [21], [28].

TABLE 6-II. AN ATTAINABLE GOAL FOR THE REDUCTION OF COST IN THE LIFE CYCLE OF SOFTWARE.

	Present Annual Cost (Millions)	Percentage of Reduction	Yearly Savings (Millions)
Design Errors	1,200	15%	180
Logic & SYNTAX Errors	90	25%	22.5
Maintenance Cost Not Attributed to Errors	210	10%	21
	1,500	15%	223.5

NOTE: Cost data above are based on an annual cost of $3 billion.

- Definition of all data inputs to each segment and data outputs.

- Test plans to test the operation of each module.

(1) Approaches to Software Design. The design process is frequently not a formalized approach. One approach, HIPO, which is described in this section has been successfully used in the development of software for large stored program controlled telephone switching machines [25]. A variety of approaches have been utilized with limited success; these approaches do provide guidelines and are certainly better than undisciplined approaches. Some of the techniques being utilized in the design process are the following [21, 30, 31]:

- Levels of abstraction, as defined by Dijkstra, provide a framework for clear and logical system design. The system is conceived as a hierarchy of abstract levels. The lowest levels are closest to the machine. Each level supports an important abstraction; levels of abstraction is a useful specification tool because it allows us to become less dependent on "nonessential" details of a particular implementation [30, 32].

- A top-down development process in which the higher level module is given as a program specifying the flow of control among certain lower level functional modules.

- Higher Order Software is a formal methodology for defining requirements for computer based systems [30]. It is based on six axioms; the utilization of such a system needs the support of a specification language and corresponding software tools. This approach is still under development.

- THREADS is a requirements-oriented methodology that defines a system in terms of units specifically keyed to required system capabilities. This system was developed by Computer Sciences Corporation.

- HIPO is a procedure developed by IBM [33]. The objectives are expressed as a hierarchical procedure where inputs and the corresponding process and resulting outputs are defined and redefined until the desired level of detail is obtained. The intermediate stages are retained.

Frequently a combination of different techniques is utilized in the design process. Unfortunately, the importance of the design phase is frequently not recognized. While these approaches or techniques have provided some improvement in the design process, there is still an urgent need for additional progress in design

techniques. This need is indicated by the high cost of errors in system design and the failure of software to perform its intended function.

(2) Potential for Improvement in the Design Process. There are two ways to approach the improvement in the design process: (1) improve the current techniques, and (2) identify new techniques. Management reviews and technical "walk-throughs" have been very useful in identifying design errors. The walk-through is a formal review technique where test inputs are generated and "eyeballed" through the design to verify its accuracy [21]. While those efforts have improved the design, too often the specifications are not consistent with the requirements. Additional research is recommended to improve the approach used in management reviews and technical walk-throughs. It may be appropriate to develop a scenario for management review and actually let management simulate the use of the system through its outputs. The essential content and format of a scenario for such a review are unknown. Some of these questions will be formulated and answered in a current effort, "Study of Engineering Practices for Communications Software".

The experience level of personnel is considered by some experts to be the most important criterion needed to ensure successful development of software [21]. Thus, there is a need to develop a technique for recording the design efforts of experienced personnel so that this information can be identified and retrieved for review [34]. More emphasis has been placed on other areas such as proof of correctness, portability of programs, and languages which assume the design is correct. Yet, the errors in design represent approximately 40% of the life cycle cost; it appears that more emphasis needs to be placed on design. It may be possible to modularize and define portions of design efforts such that they are useful in future efforts.

There is a real need to be able to verify that the specifications are consistent with the user requirements, and similarly, the computer programs are consistent with the specifications. For example, it would seem reasonable to prove that each message in a telecommunications system has been delivered. Some research is being done to prove that security policies are accurately supported by the system [35]. This effort should be extended to include the proof of functional requirements.

Design flexibility is especially important in regard to changes in requirements, particularly those occurring after a system is operational. There is need to develop a methodology that would enable a design to be described and certified in terms of functional capabilities. It would be a logical or conceptual design which could be the basis for the mapping of real software/hardware components during the implementation of a system. The usefulness of such a

design will depend on the guidance and insight it can provide for actual implementations. It is a reasonable approach for ensuring flexibility in design, and it represents an initial method to record the design efforts of experienced personnel. It is usually described in terms of abstract entities such as logical processes and virtual entities. DCEC recently completed a contract that studied the development of a logical model for communications software. This contract explored the feasibility of some specific rules and actually simulated the implementation of a simple model. There is also a need to develop a methodology for the logical design and integration of hardware and software.

In summary, there is a great need to verify that a system design is consistent with user requirements and to prove the system design has the potential to perform its intended functions. Furthermore, there is a need to express or record a design effort such that it can be easily reviewed and utilized for related efforts. More of our current research should be directed toward these goals since there is a high potential for a larger return on the investment.

b. Maintenance. There are two divergent ways to reduce maintenance cost: one way is to make it easier and less expensive to do maintenance by designing equipment which will be reliable and easy to maintain; the other way is to eliminate the need for maintenance. Unfortunately, it is not realistic to eliminate all maintenance. Even if it were, the capability is still needed to upgrade and meet the changing needs of a system. These same capabilities enhance the ability to perform maintenance. For example, detailed design and coding standards must have been established and then followed for effective maintenance and updates. Furthermore, it is predicted that the maintenance cost on real-time systems currently under development will exceed several times their development cost on existing systems (see Figure 6-3). Figure 6-2 shows that more than half of our maintenance is a reflection of poor or incorrect design.

The management process which is used to maintain a program after completion of design is called "software configuration management" [21]. After configuration control takes effect, all code and documentation forms should be accompanied with the supervisor's approval and the reason for change. The maintenance programmer and the chief programmer report to different line supervisors. The maintenance programmer should have the responsibility to verify that program modules work according to the specifications. The maintenance programmer formally agrees that the program modules are properly documented, structured in design, easily readable, and conform to all specified standards [21]. The idea is to enable the individual whose future effort is most affected by the completeness of the development to have an opportunity to review and accept or

reject the software based on his evaluation of its status [21]. Unfortunately, in a government installation the potential impact of the development effort is not likely to receive the same level of scrutiny. However, the same need exists to ensure that maintenance can be performed. This approach will increase development cost; however, it should reduce the total life cycle cost.

c. Computer Networks. The ability to communicate between different computers extends the horizon for potential approaches in software development. It also increases the need for compatible and standarized software. The ability to electronically transport and transform software into different forms enhances the likelihood of developing software that either is in a portable state or can be transformed into a portable state. Software, unlike hardware, can be transmitted as electrical signals and can be utilized in another location, which leads to uninhibited sharing of resources. The sharing of software is a tremendous opportunity for reduction of software cost.

(1) An Operating Environment for Sharing of Software. One logical approach for the identification of potential solutions for software sharing is to first define an environment that would be the most conducive for shared involvement. For example, if each member of different teams at different physical locations used identical computer equipment, an identical operating system, and the same computer language, there should be an opportunity to share the work load where the efforts are similar. Furthermore, if by chance, each functional group at different locations were assigned the required work could be divided among all the different groups and the same result achieved in a more efficient manner. Now carry this process one step further in an attempt to illustrate a need for cooperation; for example, what if this same task had already been satisfactorily completed by one or more of the functional groups in the system? Obviously, the desired software package is in existence. What should be done next? In this environment one might think of the software planner as an individual who selects the programs or program families [36,37] needed to build a software system. His task would be analogous to the designer of a piece of equipment who intended to extend his product line with a minimum of new parts. The designer would identify basic requirements and partition them into functional entities that could be supported by components already designed and tested.

Concept interchangeability is very desirable; however, this is not likely to occur unless proper emphasis and planning are focused on this issue. The designer must also recognize that there is an economical advantage from utilizing components that are in the standard product line of other organizations. The opportunities for economical gains from program families [37] are even greater than

those for interchangeable parts. For example, a portion of a software system that is already available in the form of functional modules is practically free. There may be some interface problems, but it is a tremendous opportunity for cost saving.

A question one should consider is why government organizations are not taking more advantage of this sharing opportunity. Part of the answer is reflected in the organizational structure and the level of software awareness that exists within the structure. The individual who writes programs for a particular organization probably has his own set of routines that he uses over and over. He has tested these routines, knows the basic logic, and has confidence in their reliability. The perspective is much different once the programmer is asked to use some other programmer's code. He may decide the logic is not clear and the documentation is inadequate. In fact, the programmer may decide it probably does not even perform the desired functions. Management's lack of knowledge and awareness of software issues has practically guaranteed that in many organizations very limited consideration will be given to the generation of software with a planned intent for use in multiple systems.

Besides management issues, technical needs and concerns must be addressed. For example, what information must be made available to a potential user so that he can decide if the software is useable in its current state? Once the potential for modification has arisen, then the information essential for a decision of this magnitude is considerably greater than that needed only to implement the module. It is possible that software modules should be classified such that those most likely to be utilized on a repeated basis would receive special attention in terms of documentation. What is needed is a virtual language that could be translated to a state compatible with any system that had specific functional capabilities. These software modules would still have to be tested to verify portability and capability.

Many questions need to be answered to pursue a solution along this route. For example, what definable characteristics can aid in the selection of those modules which are desirable for purposes of sharing? What information is essential to determine the utility of a program? Would a virtual machine need to be defined to clarify functional requirements needed to ensure proper mapping? Is it possible to develop a "virtual" language? Would the language be applications oriented? How can one retain information such that a user can quickly determine the availability of software to meet a need? If the cost of software is so high, why isn't the software that is already completed, tested, and verified used on repeated occasions? Unfortunately, part of the answer is no one knows how

to easily identify software to meet a desired utility and establish the extent of its portability. The potential is so great that this area of research should receive additional attention.

(2) Requirements for Protocols. In order to provide effective communications within a computer network, provisions must be made for carrying on several transactions simultaneously on a single access port. One solution is to schedule the processing of transactions on the basis of identifiers included within each message transmitted [38, 39]. This defines the network access protocol. A network access protocol should include means for the following [39]:

- Identifying destination of data on a message-by-message basis.
- Transmitting interleaved messages to multiple computers and terminals.
- Precluding the delivery of messages to unauthorized users.
- Controlling the flow of data into the network.

The methods currently used for accessing data communications are very similar on different networks. There are significant benefits to be gained in adopting network access standards [38]. This would enhance the likelihood of resource sharing and insure that computer systems could communicate with each other.

d. Programming Language Issue. Programming languages influence the process of program creation and the properties of the final program. The capability to develop a computer program on one machine and execute it on several other machines is dependent on issues relevant to the programming language.

(1) High Order Language (HOL). Using a high order language (HOL) can result in reduced cost, increased portability, and lower maintenance cost. Several issues relating to HOL for communications language need additional investigation, such as interfacing with operating systems, real-time code, parallel processing, and assembly languages. The high order languages currently available have serious deficiencies in these areas. It is possible with known technology to develop a high order language for communications systems significantly superior to those currently available.

An example of an early attempt to make expert knowledge of an application available to the ordinary user was the development of a switch configuration simulator language called a "Communications Computer Language (COMTRAN)." The purpose of the COMTRAN system was to provide Rome Air Development Center (RADC) with a communications-oriented simulator system that would accept parameter statements in a language which was convenient for test engineers to use and

produce programs that could operate the stored program element in accordance with the requirements of the engineers [40]. This software was restrictive since it was developed for a specific computer system, the 465L system [40]. The need today is for the development of knowledge based systems that are machine independent.

e. Programming Methodology. Limited advances have been made in programming methods and techniques. Some of these methods offer immediate means to reduce cost [21, 25]. They are briefly described to identify these proven approaches.

(1) Top-Down Design. The top-down approach utilizes the systems analysis concept; the bottom-up approach attempts to identify software components and to develop a software package through synthesis. The top-down approach starts with a statement of the objective and breaks down the requirements until simple components can be identified. This approach is helpful in defining functional software components required to meet the objective. Then, it is appropriate to use a bottom-up approach to develop the functional components.

(2) Modular Programming. Modularity denotes the ability to combine arbitrary program modules into larger modules without knowledge of the construction of the module. It is an accepted and widely utilized concept.

(3) Programming Team Concept. The programming team concept is an approach developed to utilize skilled personnel properly and to ensure that responsibility and accountability for software are shared by team members. It has been successfully used on large software development projects.

(4) Structured Programming. Structured programming is an attempt to reflect the structure of the design within the source statements of the computer program. Basic rules are established and followed. For example, structured code modules are restricted to a maximum number of lines. Control always enters a module at the top and leaves at the bottom. All modules are referenced by name. Branching between modules is restricted; a module either returns to its caller or moves sequentially to the next module.

f. Program Verification. It is impractical to test every path through a program under all conditions, although there are computer software packages available which aid in determining the extent of such testing. Formal verification or proof of correctness is an emerging discipline, but currently only relatively small programs have been verified using such techniques. A computer program is considered correct if it functions as intended. For example, if a program is developed to perform a task described by a flow chart,

then a proof of correctness would guarantee that the program performs the logic that was outlined in the flow chart, or more accurately, as it was interpreted by the programmer. Likewise, if a program is developed from a set of specifications, it is not just the specification which dictates what will be proven, but the programmer's interpretation of the specifications.

Current methods for proof of correctness require the programmer to develop appropriate assertions to insert within the code and/or the data declarations. Since the proof of correctness is dependent on the validity and appropriateness of the assertions, if the assertions do not truly reflect the intent of the proof, the proof may not provide the assurances sought and expected. Consequently, research is being performed which allows the programmers to use assertions as part of his program specification. The problems in proof of correctness have been simplified by a new technique called data abstractions [41] which are assertions to prescribe the extent to which certain data may be used within a program or subroutine. Thus, as long as these abstractions are followed, and the abstractions have been verified, the program is correct. A compiler may be used to enforce compliance with the abstraction [41].

Important considerations regarding the proof of correctness of software are summarized in the following statements:

- The proof of correctness cannot be based on someone's interpretation of the specification, which is not necessarily the intent of the specification. Specifications need to be expressed in a form that eliminates ambiguity. Additional research is currently being performed to achieve this capability.

- Proof of correctness procedures must be based on a set of assertions sufficient to guarantee a proof. Research is being conducted on interactive techniques to provide such a capability.

- The capability to prove production size programs is still in an experimental state; furthermore, there are significant requirements within DoD in security related areas such as "BLACKER" that are dependent on this capability. Researchers have experienced success in proving programs as large as one thousand lines. However, the researchers have been allowed to choose for verifying only functions which could be programmed in the subset of a programming language deemed verifiable.

- There is a need to extend the proof of correctness techniques to handle computer programs that are executing in a multi-processor environment.

- The proof of correctness capability can be justified by the following:

  - The need to enhance program portability and reliable use of program libraries by using the compiler to ensure that library programs and/or subroutines are properly used.

  - The high cost of maintenance in real time systems.

  - The potential loss of human life or wasteful expenditures that can be a result of errors in software (e.g., space flights).

  - The need to develop secure systems that include software components.

  - The need to prevent duplication of software efforts.

In the last 2 years considerable effort has been devoted to the development of a language whose structure would aid in the development of such a proof. The University of Texas has developed such a language and a methodology and is currently in the process of developing a compiler for the language. Similar research is being performed by Carnegie-Mellon University, USC Information Science Institute, MIT, and others.

Even though Dijkstar has correctly and succinctly pointed out that "testing proves nothing about the absence of errors only their presence" [42], he does not conclude that testing is an obsolete approach. There still is a need to design and develop programs such that testing can be done effectively [43]. No one has suggested verification as a replacement for testing; however, one can expect improvements in the method and control exercised in testing. The high cost of software maintenance justifies significant expenditures to ensure that a program design is implemented correctly, and it seems reasonable to anticipate significant results within the next 2 to 5 years.

g. Program Documentation. Proper documentation is an important step in reducing maintenance cost and providing the capability for effective and efficient updates. Program documentation is one of the most arduous tasks of the programmer; hence, management attention is required to ensure that programs are properly documented. It is important that the programmers have not only adequate assistance to minimize the required effort, but they also need encouragement and control to ensure that the task is completed. Documentation should not be prepared in minute detail or in a form in which it cannot be easily updated. It is better to have less but accurate documentation [21]. There is a serious need to provide documentation

to analyze programs automatically to determine if they meet the requirements of a prospective user. Obviously, documentation is essential for effective maintenance.

(1) Manual and Computer Assisted Narrative Documentation. The capability to generate meaningful narrative information which supports program development is an area that needs more investigation. Some facilities have developed interactive software packages which request information considered essential for documentation. This procedure guides the programmer during the documentation process and makes the task less laborious. Since timeliness of documentation is important, this procedure integrated into the coding cycle would be beneficial.

(2) Program Librarian Functions. A librarian is needed to ensure proper procedures are followed for updates and changes. It is imperative that appropriate documentation be provided for new library entries and changes in the current programs. The librarian assures that the program library remains a useful and reliable entity to the user. The librarian is considered an essential member of the team in the chief programmer team concept.

h. Personnel. The skill level and learning ability needed to develop and/or maintain real-time software have been greatly underestimated. It was pointed out in a recent report [44] that DoD has insufficient software expertise at all levels, and retention of skilled software engineers is hampered by an attitude that programming is a job for a low-paid technician. In another report [21] it was noted, "The most important single factor which determined the different development rates is the experience level of the designing programmers and supervisors." The large variance in the productivity of individuals in the development of software makes it a critical issue. There is an urgent need to measure productivity and identify those elements that are critical. The importance of personnel in software development is reflected in the fact that 70% of the cost of software is directly attributed to personnel cost [19, 44].

Current studies show a high correlation between an individual's productivity and the reliability of the software [19, 22], i.e., more productive individuals produce more reliable software. Relevant past experience is important. The immediate supervisor on a project should have programming experience. Suitable training and experience are imperative for specialized programming such as that required in the development of communications systems software. The minimum amount of exposure and training required before programming personnel can develop communications software is not well understood. This information would be beneficial in both the selection of personnel and the evaluation of a contractor's capability to perform a task.

i. The Role of Management. Management is the operational arm that must take the technical capability and focus it on the problems of software development. There is need for management involvement in the following [23].

- For proper validation of requirements of a new system it is necessary to perform a limited amount of preliminary design as well as proper analysis. Management should ascertain that critical design features that cannot be modeled are actually built and tested to ensure feasibility. The Defense Systems Acquisition Review Council, which is required to review any system over $50 million, is vague on the formal requirements for the validation phase of the acquisition process; these requirements should be amplified and extended.

- There is need to increase the visibility and understanding of major software components by putting them on a par with hardware components. This visibility should be maintained at all types of reviews and in configuration control related action.

- The abstract nature of software makes it difficult to measure progress; hence, formalizing the design and implementation steps is even more important. It is also important that each milestone has associated with it a deliverable; otherwise it is meaningless.

- Several contractors have stated that a formal development plan is the most important single management document for major software systems. It should be required as part of the bid package on full-scale development contracts.

- The use of proven engineering practices and disciplined program practices should be specified in the Request for Proposals. There is a tendency to leave such requirements out because they might increase the cost; however, the minimum total life cycle cost of the software is the real goal and these techniques must surely be used to meet such a goal.

- In contracting for a major software development it is important that the selected contractor has the requisite experience and capability with modern software tools. This is extremely important consideration in the selection of a contractor.

- The Request for Proposal should require the bidder to define an integration and test plan and identify the supporting elements.

- Special management attention is needed to create sufficient priority to ensure that qualified persons throughout the service organizations are assigned to key positions in the program management organization.

- It is critical that a software maintenance [21, 23] agent be identified and consulted during the validation phase of a project. He should follow the project from development to operational status.

3. AN APPROACH FOR THE REDUCTION OF SOFTWARE COST

The need for cost reduction in software development and maintenance has led to a recognition of the requirement for the development of an overall software engineering package for communications software. Such a software engineering package will be utilized during all phases of the life cycle of software for communications systems, hence, enhancing software development and improving the ability of software to be easily maintained, updated, and transferred from project to project or computer to computer. Also, inherent in the system is the ability to ascertain a confidence of correctness and security in the software product. The purpose of this section is to outline elements of such a software engineering package.

Several existing software engineering packages [44, 45, 46] are directed at goals similar or related to a software engineering package for communications systems. The contents of a software engineering package is dynamic and should reflect the latest proven technology. One of the objectives of the software engineering package is to be able to update the package and to reflect advances in technology. Before examining some specific requirements of such a package it is important to review elements included in the life cycle of software (see section VI, 1.b).

A software engineering package must support the total life cycle of the software. An effective software engineering package for communications systems could have the following components:

- A method to identify essential requirements at a level such that hardware/software tradeoffs can be realistically considered in long range planning -- a modeling of processes.

- A higher-level language that is specifically oriented toward communications systems in order to facilitate economical software development and maintenance. This is the Communications Oriented Language (COL) [47].

- A compiler to translate portable COL statements into executable code.

- A means to provide and then verify or prove that a system meets the desired security requirements.

- An operating system for communications systems (networks) that can support COL programs at multiple levels of security in an environment that appears machine independent to users.

- A method or procedure to validate software to ensure that it performs its intended functions.

- Based on the prevailing level of technology, a set of updated and proven software tools to support software design, documentation, validation, specification, and other activities required in software development and maintenance.

- An inherent capability for accommodating changes required as a result of varying applications and/or development of new levels of technology.

- A set of software engineering practices and guidelines that ensures intended requirements are met in a consistent manner.

- A plan containing guidelines for the management of software projects in a network environment such that proper control, expertise, and software tools are utilized. This should ensure that production and maintenance are economical and that the software is reliable.

- An on-line data management facility that provides an external capability to monitor, measure, analyze, and evaluate a software project.

- A model or approach to estimate software cost in order to evaluate different alternatives. The model should also estimate the relative value of different practices and their influence on software cost.

4. PROGRAMS FOR SUPPORT OF A SOFTWARE ENGINEERING PACKAGE

There are both in-house efforts and contractual arrangements planned and in progress that support the communications software engineering package. These efforts are briefly described in the following paragraphs. Figure 6-4 represents a dynamic plan which is our ultimate goal.

a. Current and Prior Software Efforts. The efforts related to software prior to FY76 were focused primarily on defining a communications-oriented language (COL) that could be efficiently utilzed for development of communications software. Even though plans for a more encompassing software engineering package had been initiated earlier, very little effort was expended toward this goal until FY76. The following efforts are either recently completed or in progress:

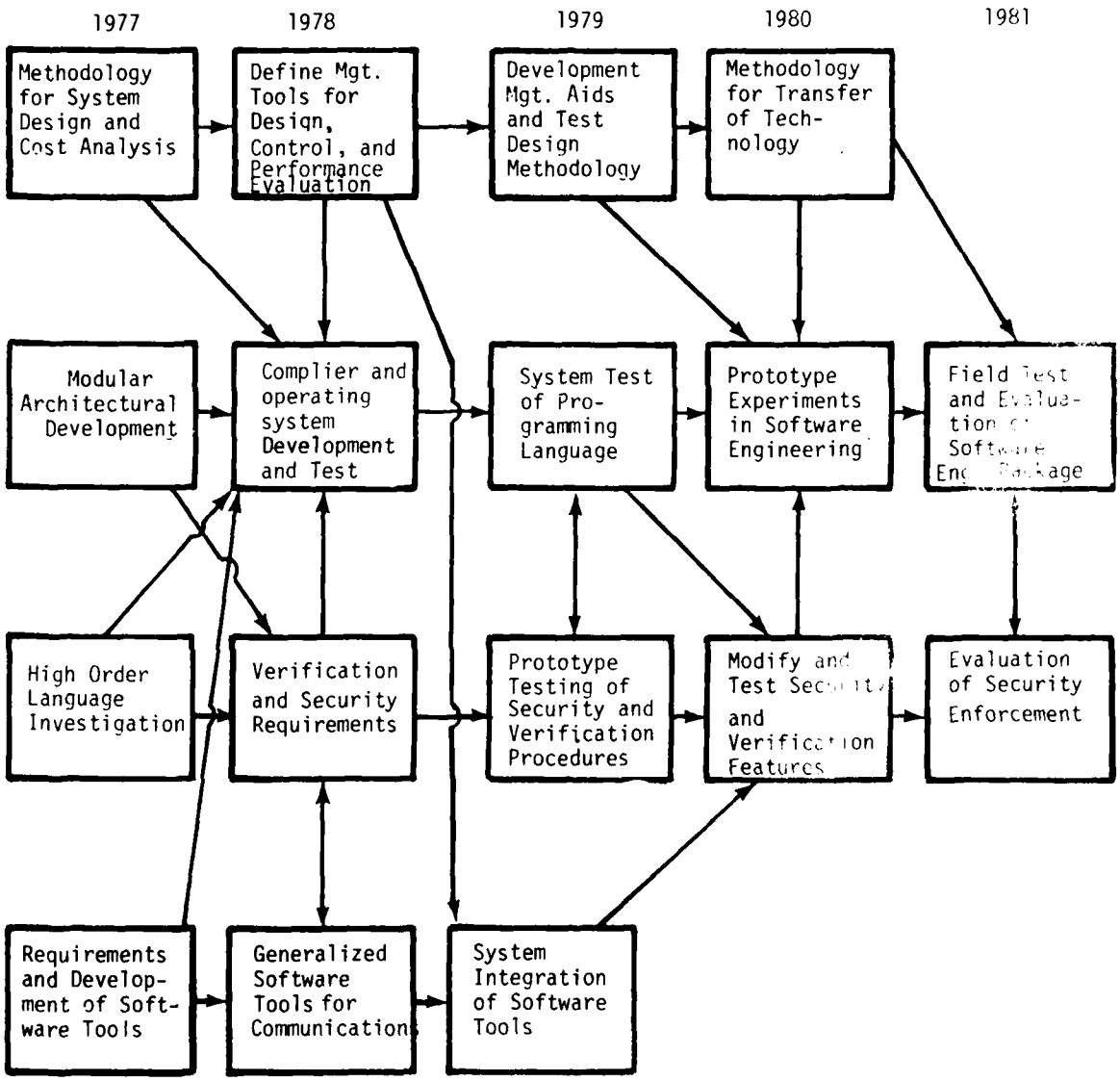


Figure 6-4. Research and Development Essential to Attain a Significant Reduction in Software Cost

- Guidelines for Defense Communications System Software Production. This contract is intended to review current guidelines and practices needed to assist in the economical development of communications software. The contractor is required to identify elements within communications systems that can have an impact on cost related to software.

- COL/Compiler Development. This effort analyzes the requirement for a COL, identifies the benefits obtained from using a COL, describes a syntax for a COL, and outlines a complier organization. Furthermore, this effort will provide DCEC sufficient information to finalize its position on the syntax for a COL. This was a competitive award to Bolt Beranek and Newman, Inc., in FY 75, with a sole source extension in FY 76/7T.

- Higher Order Language Investigation. The objective of this effort is to define the capabilities required of a higher order language for producing application software for the Unified Digital Switch and using these requirements to develop a highly efficient, reliable, and easy to use programming language for use in developing this software. This language is being developed by incorporating all necessary modifications and deleting all unnecessary constructs from an existing higher order language. This is a contractual effort under the cognizance of RADC.

- Modular Architecture Development. A modular interconnection architecture concept will be evaluated for use on future signal processing and switching equipment. This effort provides information vital to architectural concepts being developed for IASA (Integrated AUTODIN System Architecture), future switching equipment development, and communications processor equipment. It is a sole source contract to Collins Radio Corporation in FY 76/7T.

- A Communications Software Development Package. The Communications Software Development Package (CSDP) provides a software environment in which the application programmer prepares, tests, validates, maintains, and simultaneously documents his programs. Using the CSDP, he may call upon any one of the various support software packages to aid in the preparation of finalized communications processing programs. This is a multiple year contractual effort under the cognizance of RADC.

- The Communications Switching Operating System. A study will be conducted to evaluate current operating systems and their usefulness in a communications environment. These systems will be categorized based on the service functions they perform. This is a contractual effort that is under the cognizance of RADC.

- Performance Evaluation of Software Candidate Structures. Burroughs Corporation under contract to DCEC has developed and recommended a generalized software structure for executive systems. There are some obvious benefits from such a structure; however, the current software structure is not efficient. There is a need to model the software structure so that bottlenecks can be identified and eliminated. Ultimately, the structure will be redefined. Continuation of this effort is currently planned as an in-house effort.

b. Long Range Plans. A long-range plan has been defined in order to reduce software costs. This plan contains six general areas of effort:

(1) Software System Modeling and guidelines for DCS software production.

(2) The development of a programming system which consists of a communications oriented language (COL), a compiler for the COL, and a communications switch operating system.

(3) A communications software development package.

(4) A methodology for configuration of a modular architecture development which includes consideration for software/hardware tradeoffs for language interfaces.

(5) Multilevel security design and integration into the Defense Communications System.

(6) The consolidation of software engineering tools and concepts into a single and useful entity, namely, an automated software engineering package.

c. Candidates for In-House or Contract Support. The six areas of interest will be supported by either contracts or in-house projects. The in-house projects are frequently extensions or complementary efforts to contractual results, and represent a crucial effort which can be met with internal resources. The candidate projects, which will be phased over a 5 year period, are the following:

(1) A study of the portability of Communications Oriented Languages.

(2) Development of models for performance evaluation of software candidate structures for executive systems.

(3) The development and installation of basic computer networks to be used for research facilities (END, ARPANET, Secure Communications Node).

(4) An evaluation of the usefulness of meta compilers for elimination of machine dependencies in languages.

(5) A conceptual study to determine feasible approaches for design and implementation of software with multilevel security requirements.

(6) The development of an annotated bibliography on software verification and certification.

(7) A review of software standards currently enforced by DoD.

(8) An outline of essential requirements for a software acquisition management plan.

(9) A concepts paper on implementation of computer networks for communications systems.

(10) Recommendations for software standards to support communications systems.

(11) A prototype model that represents the skeleton of the needs for project monitoring and evaluation of software.

(12) A study to evaluate and recommend the proper utilization of generalized data base management systems such as TOTAL in the development, control, and management of software tasks.

(13) An updated plan for reduction in software cost which contains the following:

(a) Recent achievements
(b) Current research efforts
(c) Long-range plans
(d) Milestones
(e) Essential resources
(f) A summary of other efforts
(g) An assessment of the likelihood of success and the respective benefits of each planned activity.

(14) A definitive report on measurements that are essential for successful implementation of a software engineering package.

(15) A report that outlines current software/hardware tradeoffs in communications systems and expectations based on current technology.

(16) A field study of problems currently encountered with software maintenance.

(17) Specification for the development of a machine-aided analysis of communications specifications.

(18) Specifications for a "software first" machine.

(19) A DELPHI Study to identify which research areas offers the best opportunities for a reduction in software cost.

The in-house projects will be reviewed each year. Progress will depend upon the availability of personnel.

5. COMMENTS ON THE SOFTWARE PROGRAM

The development of a software engineering package is a consolidation of many capabilities into a single entity to ensure all the necessary factors are considered in a timely order. However, the development of a software engineering package does not ensure it will be utilized. Furthermore, the development of some elements such as the cost models for software, a plan for transfer of software technology into the field, a plan for data collection to support software models, management aids, techniques for increased productivity, and a methodology for design (see Figure 6-4). However, it is currently planned to integrate these requirements into current programs.

It is easy to identify specific examples and/or procedures that reflect DCA limitations in some of the areas mentioned in the preceding paragraph. For example, the current approach for estimating the cost of telecommunications equipment does not separate hardware and software costs. If two identical switching mechanisms were used one would expect to pay for each piece of hardware; however, the software for additional systems may not require any additional expenditures except for installation. Before one can expect to control cost, one must be able to identify the cost of the operational components and determine the incremental cost expected for related or identical systems.

There are certain proven approaches for development of software that have consistently reduced the life cycle cost of software. However, these approaches are frequently not a requirement placed in the S.O.W. because the Government representative has no way to justify or estimate the effect of a particular approach on the development cost. Current budgeting practices do not take into consideration the impact of software maintenance. Indirectly, upon project approval, there is a commitment to maintain the system which is a greater expense than the development cost. The ultimate result is that proven technology is not utilized. Hence, there is a need for a method to transfer proven software technology into the field.

Many experts [21, 25] agree that maintenance represents more than one half (it has been estimated as high as 75%) of the life cycle cost of software. Furthermore, since 80% of the maintenance cost is directly attributed to design errors [25], there should be more

emphasis placed on design methodology. One question that has been reviewed on occasion is whether there should be a software maintenance center or whether maintenance should be contracted. However, it is more appropriate to consider the effect of a design/ maintenance center.

Even though 70% of the software cost is directly attributed to personnel [19, 44], very little has been done to increase the productivity of people involved in the production of software. How much work an individual should be expected to complete in a unit of time needs to be determined to evaluate personnel and make accurate cost estimates. The level of achievement of people in software has been measured to vary as much as 26:1. Undoubtedly, this is a fertile and potentially rewarding area of study.

In summary, many of the current efforts in software are primarily directed at meeting specific requirements. For example, the BLACKER program requires the capability to develop provable software. Hence, considerable expenditures are being made to achieve this goal. It is much easier to justify the expenditure of funds in order to meet technical goals that are essential for long term objectives. It is difficult to justify expenditures that will increase the immediate cost even though the total life cycle cost will be significantly reduced. Nevertheless, if significant achievements are expected in the reduction of software cost, there must be a willingness to pay more in the near term and wait for the rewards in the future.

VII. DYNAMIC STABILITY

1. DEFINITION

The dynamic stability of a communications system can be thought of as the resistance of a system to unstable oscillations brought about by conceivable failure modes. It is a function of both transmission and switching subsystems and of the user and control elements. Dynamic stability is addressed because it is a direct measure of the performance of a communications system, this performance being affected by such failure modes as equipment faults and transmission media outages, and the propagation of their effects. It is these effects which can lead to unstable oscillations within the system thereby causing a measure of instability. The mechanisms for preventing dynamic instability encompass information flows between and among these subsystems and elements as was discussed in section II.

2. PROBLEM HISTORY

A simple problem is offered that illustrates both the dynamic nature of the DCS and a mode of instability. The block diagram of the transmission subsystem affected is shown in Figure 7-1. The problem was a loss of the signal from which timing was extracted. The signal from the FDM to the USC-26 group modem experienced severe degradation resulting in a very low signal level being used for timing purposes. The group modem, unable to discern the correct timing information, transmitted a pseudo-random pattern at a voice frequency corresponding to 50 kb/s. The resulting signal varied in frequency so that it appeared to the A/D device that a number of different signaling tones were being generated. The A/D device amplified the received signal and clipped the peaks resulting in a pseudo-digital bit stream input to the FTC-31 switch. Because of the frequency variation at the output of the group modem, the FTC-31 incorrectly interpreted the data stream as a number of different signaling tones. However, these tones were either not in the correct set of signaling tones or were not of a format discernible by the switch as valid or invalid. As a result, the FTC-31 sounded a major alarm and by locking up its matrix, ceased operation completely. This is a case where a fault (the loss of timing information), needlessly propagated caused a subsystem to fault, resulting in system instability which caused premature shutdown of the switch.

3. KEY SYSTEM ISSUES

The key issues in dynamic stability are timing, synchronization, communications security equipment, and subsystem fault isolation/propagation.

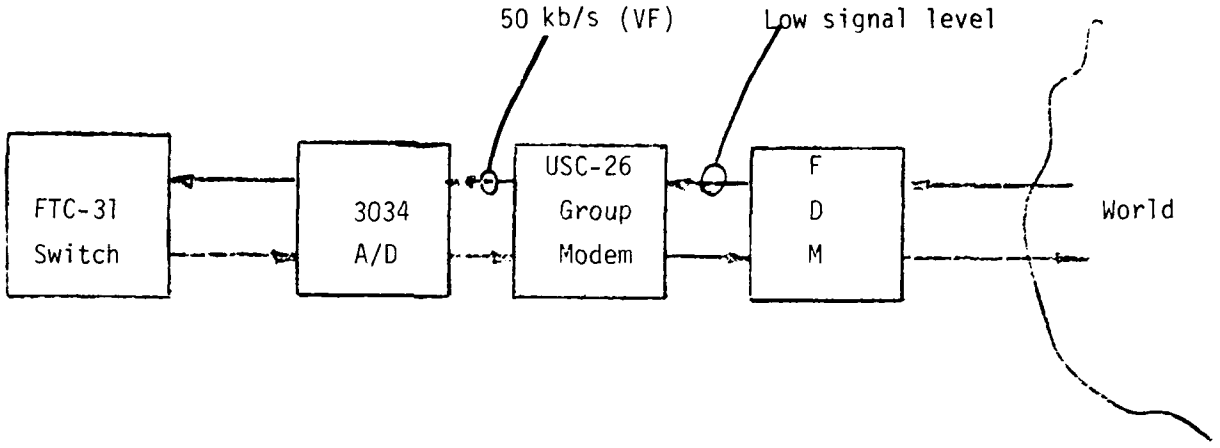


Figure 7-1. FTC-31 Synchronization Problem

a. DCS Interim Timing Subsystem. The interim DCS timing subsystem will provide initial network and station timing equipment and techniques for all digital transmission and switching requirements, including synchronization, in the transitional period of 1980-1990. A network timing proposed for the interim DCS is to utilize station clocks located at major nodes, and to derive timing from transmission equipment at minor nodes. A major node is defined to be a node with switching function, high density transmission requirements, or peculiar transmission media, e.g., troposcatter. Minor nodes have none of the attributes of a major node.

(1) Timing Equipment. The timing source, while unspecified, may comprise of independent atomic clocks, LORAN-C receivers with quartz clocks, or other similar combination of timing techniques. The performance of the timing source, however, can be specified in terms of stability. No attempt is made to discipline clocks between nodes. The timing subsystem, in addition to the clock, will include frequency synthesizers, distribution amplifiers and buffers.

(2) Timing Performance Requirements. Timing performance is characterized by two outage sources, equipment failures and the loss of bit count integrity (BCI) due to timing slips. Unavailability of equipment is determined in terms of mean time between failures (MTBF) and mean time to repair (MTTR) parameters. Table 7-I summarizes the unavailability calculations for the timing subsystem for the DCS reference channel defined in reference [48]. The higher level buffer refers to buffer placement at the bit stream output of the radio. Buffer placement at the lowest channel where a synchronous interface appears is termed the lower level buffer.

Outages due to slips occur when a buffer overflows or is depleted. Loss of bit and frame synchronization are other outages but are not included in Table 7-I. The outage caused by buffer excursions is characterized by the mean time to timing slip (MTTS) and mean time to recover timing (MTRT). Resynchronization caused by this timing failure can be expected to be approximately 0.5 sec for non-satellite circuits and up to 1.5 sec for satellite circuits. An objective for MTTS is 24 hours for the global DCS reference circuit [48]. Table 7-II shows the allocation of this 24 hour MTTS to each of the reference circuit sections. Note that the individual section MTTS values are characteristically larger than the overall MTTS value.

(3) Buffer Lengths. Buffer lengths are calculated as a function of the total accumulated time difference between two adjacent clocks, the propagation delay variations, buffer reset period, and the bit rate of the data read into the buffer. Table 7-III displays the buffer length requirements, in bits, to provide the MTTS allocations in Table 7-II. Any two clocks are assumed to be at most 2 parts in 10^{11} of each other. Propagation delay variations are assumed for line of sight and

TABLE 7-I. ALLOCATION OF TIMING SUBSYSTEM EQUIPMENT UNAVAILABILITY

	MTBF (HRS)	MTTR (HRS)	EQUIPMENT UNAVAILABILITY FOR DCS REFERENCE CHANNEL
1. Higher Level Buffer Configuration			
a. Station Clock and Associated Hardware	100,000	.5	7.2×10^{-5}
b. Buffers	100,000	.5	
2. Lower Level Buffer Configuration			4.8×10^{-5}
a. Station Clock and Associated Hardware	100,000	.5	
b. Buffers	3,500	.5	

TABLE 7-II. ALLOCATION OF MTTS FOR DCS GLOBAL REFERENCE CIRCUIT

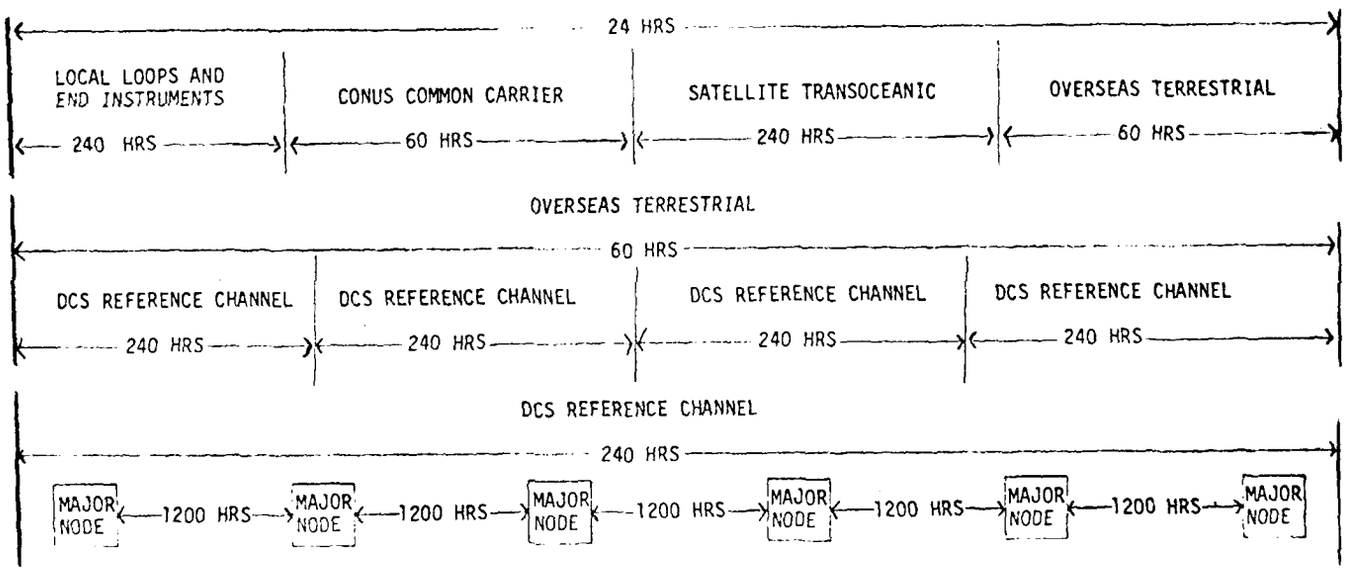


TABLE 7-III. BUFFER LENGTH REQUIREMENTS FOR THE DCS REFERENCE CHANNEL

BIT RATE (Mb/s)	BUFFER RESET PERIOD (HOURS)	BUFFER LENGTH (BITS)
0.056		2
0.128	240	4
0.256	(LOWER LEVEL)	8
0.512		16
3.232		560
6.464		1120
9.696	1200	1680
12.928	(HIGHER LEVEL)	2240

troposcatter to be 10 nanoseconds at 30 miles and 400 nanoseconds at 100 miles, respectively. The buffer reset periods are 240 hours for the lower level buffer location and 1200 hours for the higher level location. Assumed bit rates are given in the table. From the buffer length analysis it has been found that the propagation delay variations have negligible effect on the total accumulated time difference when compared to the clock time difference.

(4) Transmission Subsystem Timing. External timing will be accepted at the radio and all levels of the multiplex hierarchy of the DCS transmission subsystem (i.e., DRAMA). Figure 7-2 shows the transmit timing diagram for a major node. The clock distribution points are indicated. Figure 7-3 shows the receive timing distribution for DCS major nodes. Again clock distribution points are shown. This figure indicates synchronizing buffers at the lower level, and alternate buffer locations at the higher level. Note that in either case, for buffer placement, data is read into the buffer using recovered timing from the data stream, and written out of the buffer under local clock control.

For minor DCS nodes, Figure 7-4 and 7-5 indicate the timing distribution for the transmit and receive sections of the transmission subsystem, respectively. On the transmit side of the transmission medium each equipment will use its own internal time base. Exceptions to this usage are: the key generator (KG-81) which will accept timing generated by the radio or multiplexer on its encrypted side and furnish this time to its subordinate multiplexer; the radio (being synchronous) which will provide timing to subordinate multiplexers; and the level 1 multiplexer which will provide timing to synchronous equipments with which they interface to clock data out of the synchronous device. In the receive direction, Figure 7-5, equipment timing is provided by the timing derived in the radio.

(5) Transmission/Switch Timing Interface. The transmit and receive configurations of the timing interface between DCS transmission and AUTOSEVOCOM II elements are shown in Figures 7-6 and 7-7 respectively [49]. The switch shown is the AN/TTC-39 specified for the AUTOSEVOCOM II program. In the transmit configuration, the node clock supplies timing to the switch and each transmission equipment, with the exception of the loop group multiplexer (LGM) and trunk group multiplexer (TGM), which will receive timing from the switch.

In the receive configuration, the node clock provides the required timing for nearly all of the equipment. Some equipments however, will receive timing from adjacent equipment such as the LGM and TGM, as shown. Diphase and non-return-to-zero (NRZ) timing extraction are discussed in reference [49].

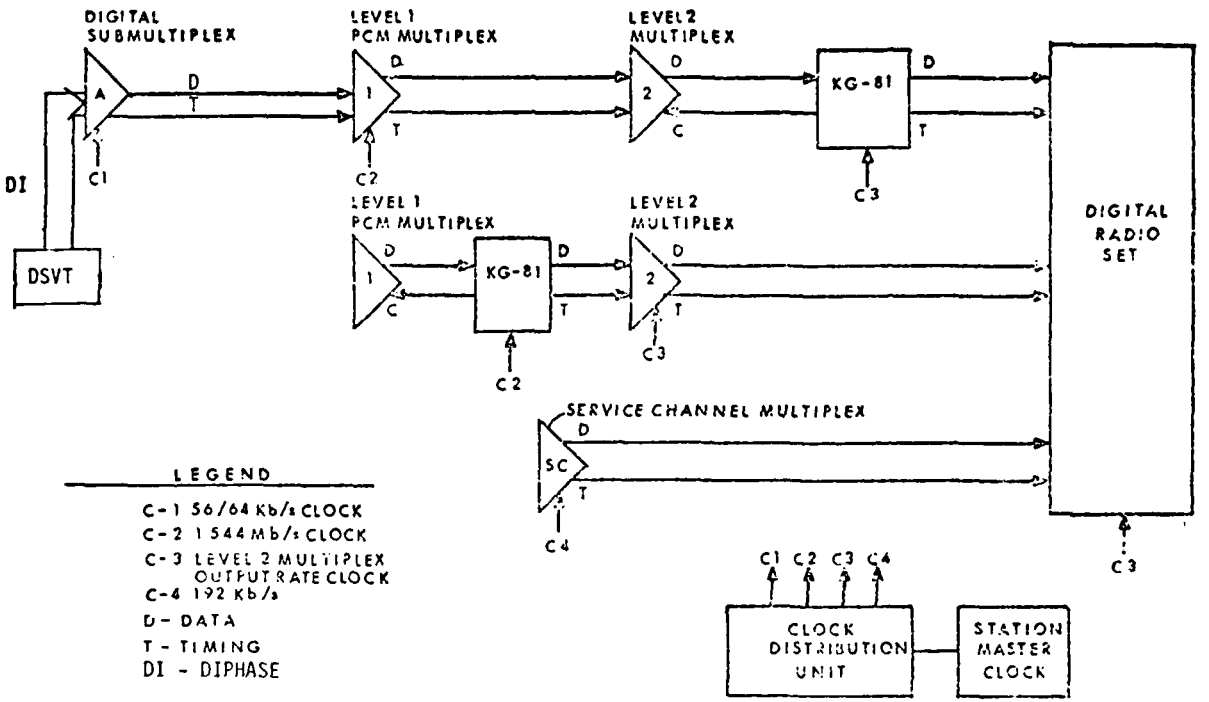


Figure 7-2. Major Node Transmit Timing Diagram

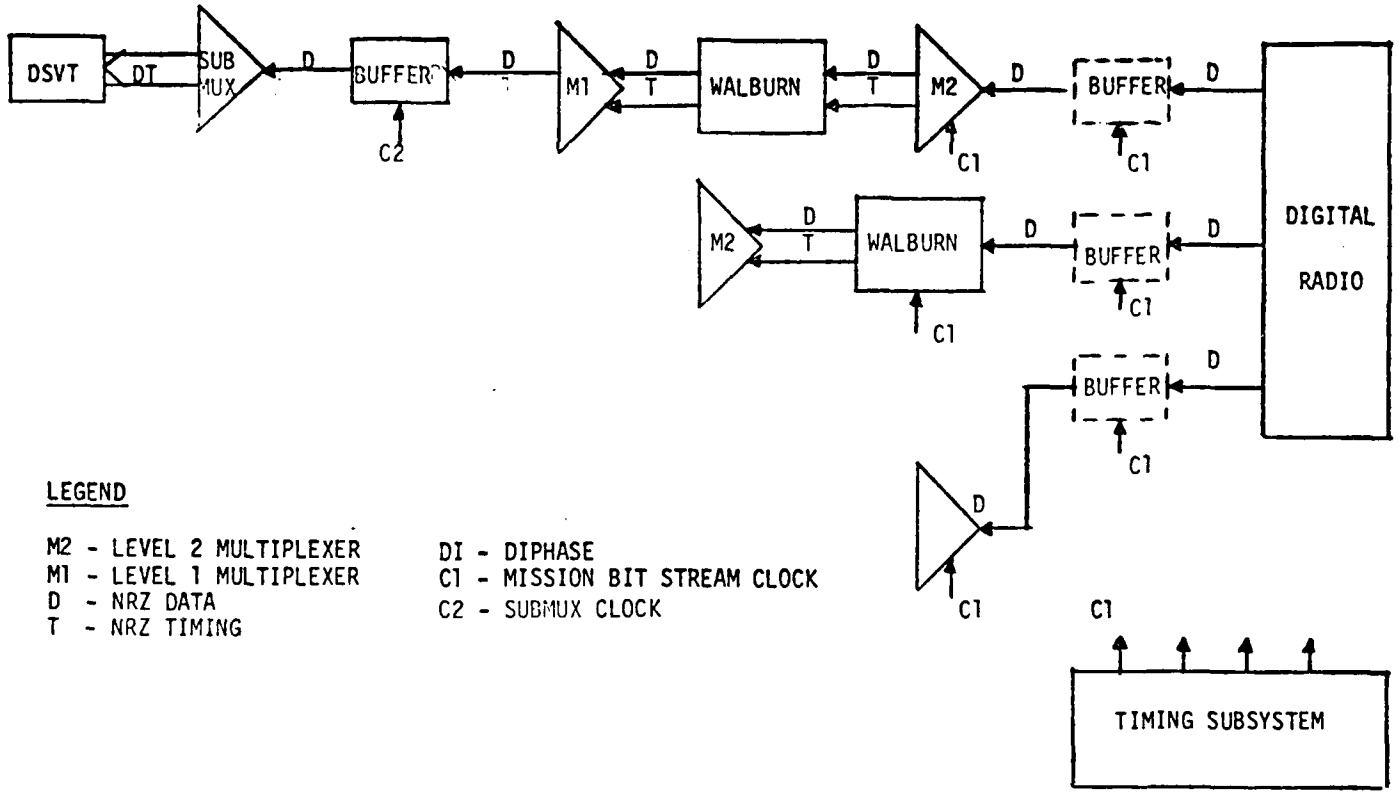
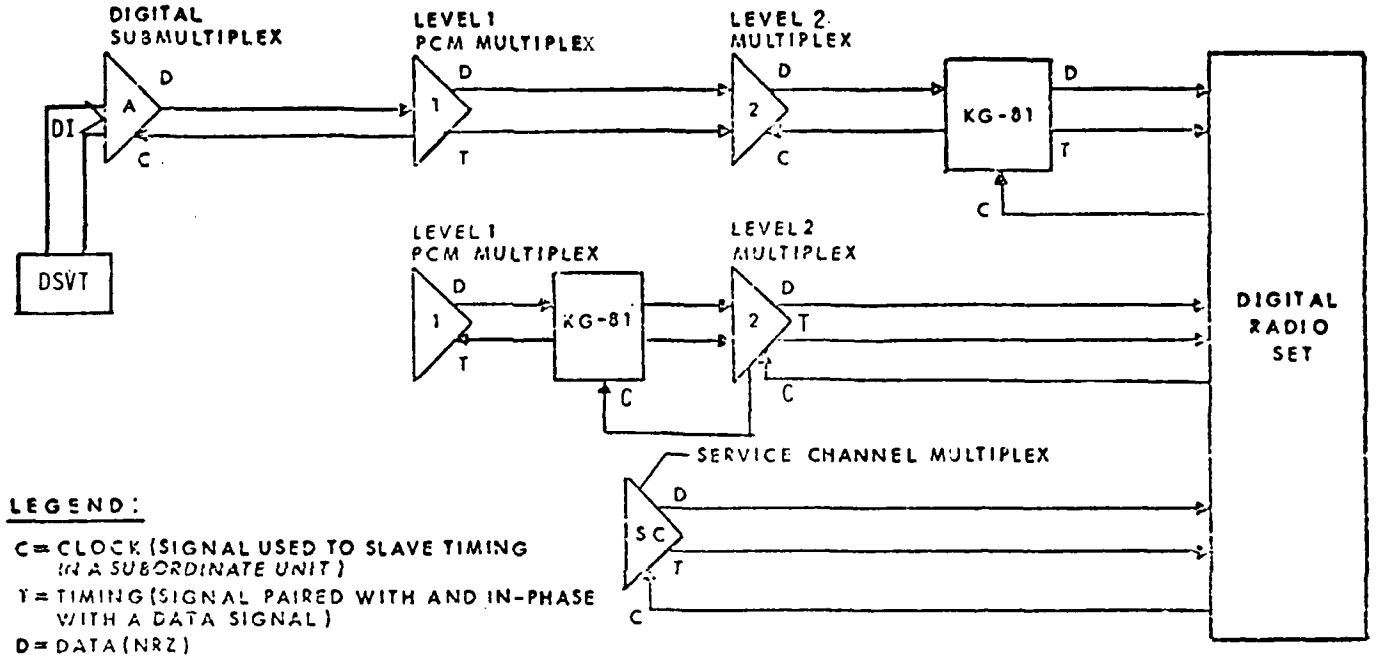


Figure 7-3. Major Node Receive Timing Diagram



LEGEND:

C = CLOCK (SIGNAL USED TO SLAVE TIMING IN A SUBORDINATE UNIT)
T = TIMING (SIGNAL PAIRED WITH AND IN-PHASE WITH A DATA SIGNAL)
D = DATA (NRZ)
DI = DIPHASE

NOTE:

DIGITAL RADIO TERMINAL AND PCM MUX USE OWN INTERNAL TIME BASE.

Figure 7-4. Minor Node Transmit Timing Diagram

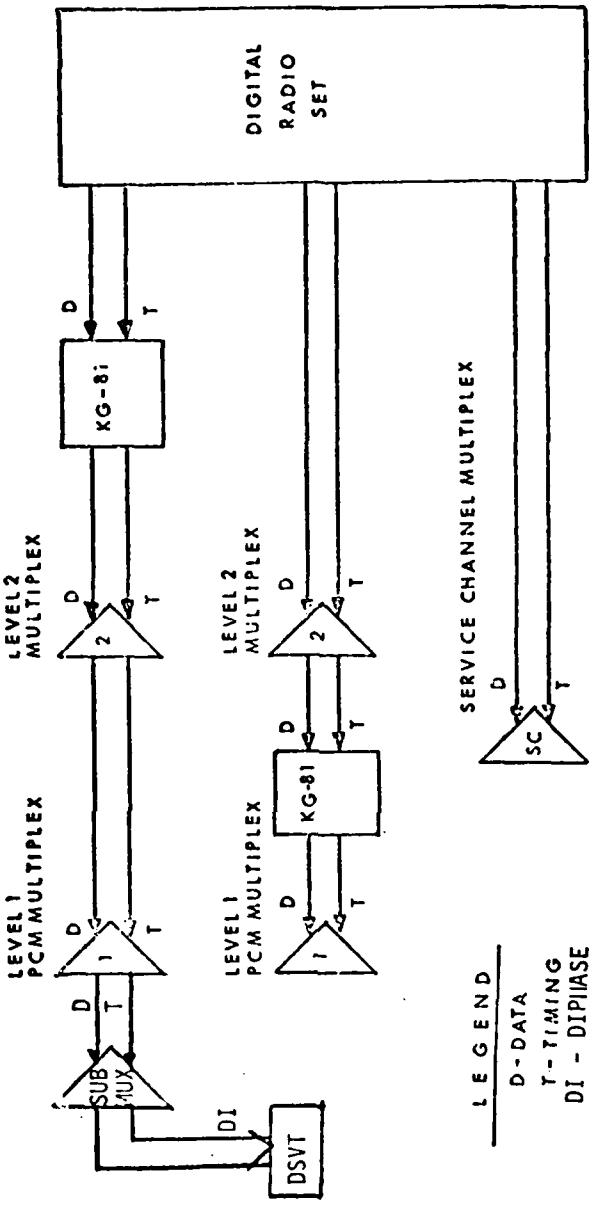
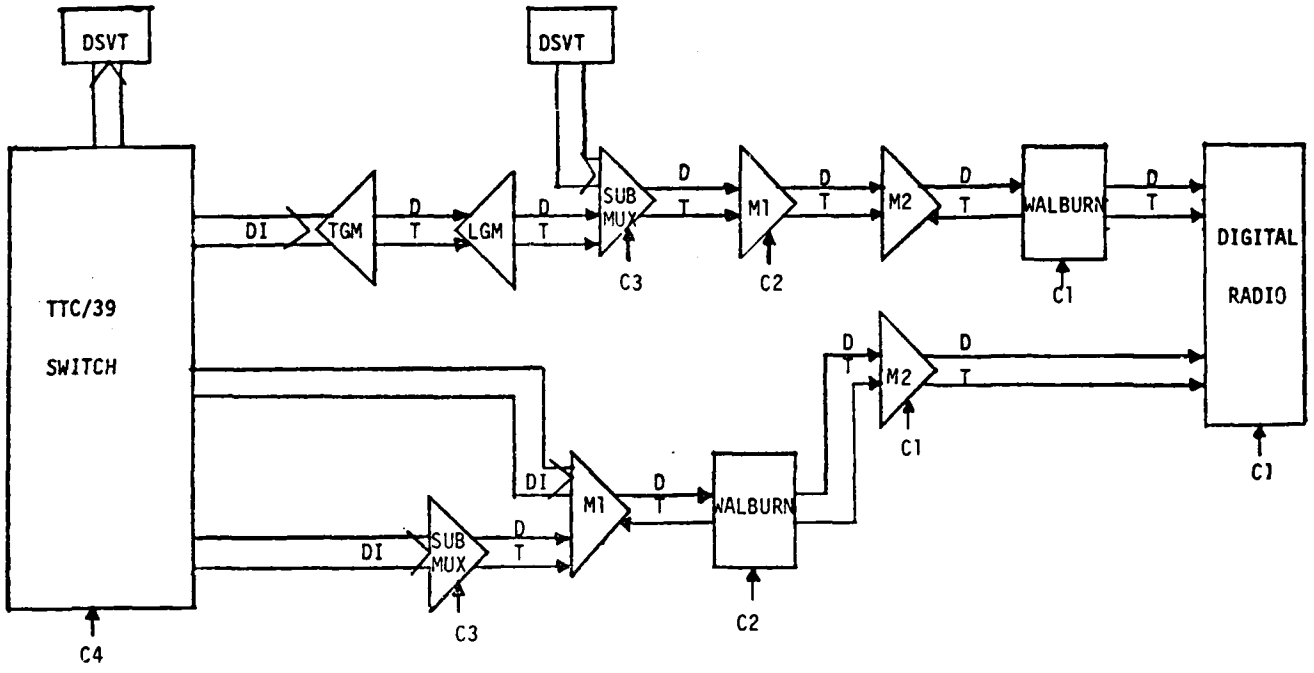


Figure 7-5. Minor Node Receive Timing Diagram

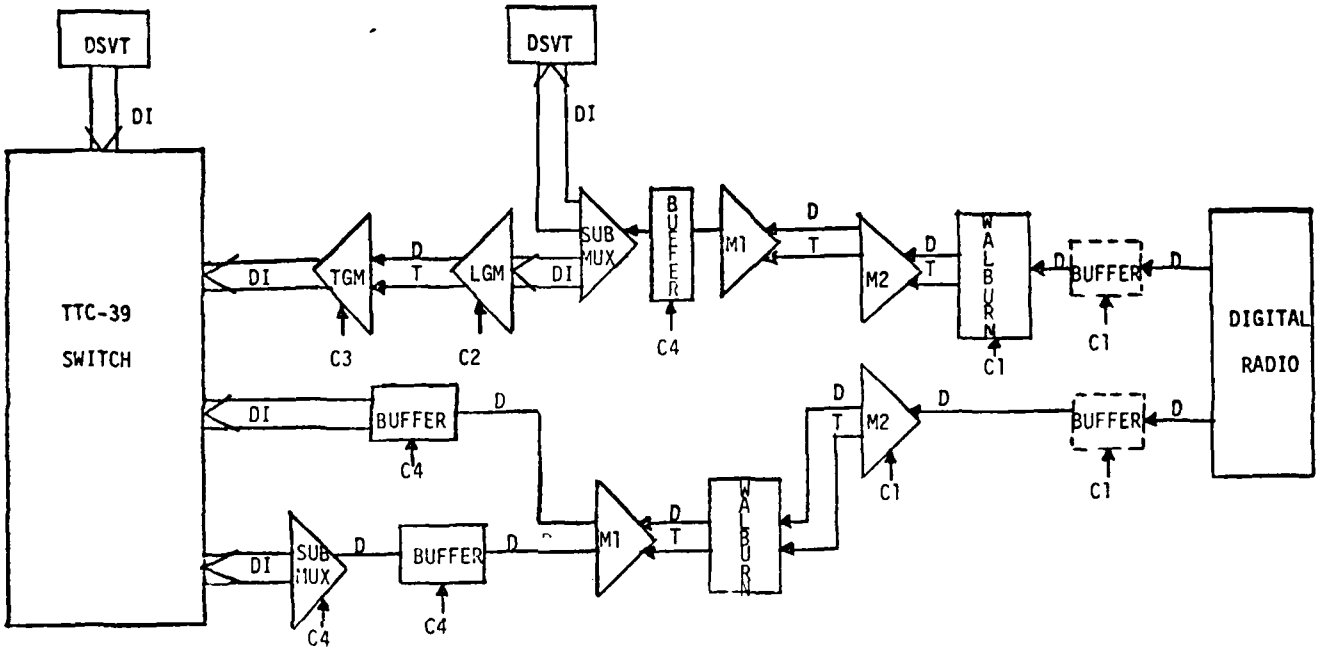


LEGEND

M2 - LEVEL 2 MULTIPLEXER
M1 - LEVEL 1 MULTIPLEXER
LGM - LOOP GROUP MULTIPLEXER
TGM - TRUNK GROUP MULTIPLEXER
D - NRZ DATA
T - NRZ TIMING

DI - DIPHASE
C1 - MISSION BIT STREAM CLOCK
C2 - 1.544 MB/S CLOCK
C3 - SUBMUX CLOCK
C4 - TTC/39 CLOCK

Figure 7-6. Transmit Timing for AN/TTC-39 Transmission Interface



LEGEND

M2 - LEVEL 2 MULTIPLEXER
M1 - LEVEL 1 MULTIPLEXER
LGM - LOOP GROUP MULTIPLEXER
TGM - TRUNK GROUP MULTIPLEXER
D - NRZ DATA
T - NRZ TIMING

DI - DIPHASE
C1 - MISSION BIT STREAM CLOCK
C2 - LGM CLOCK
C3 - TGM CLOCK
C4 - SUBMUX CLOCK

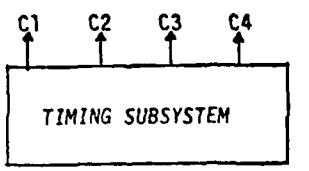


Figure 7-7. Receive Timing for AN/TTC-39 Transmission Interface

(6) Timing Sources. Network timing with some reference distribution or master/slave configuration is considered to be the goal of the future DCS timing subsystem. Candidate subsystems have been developed and analyzed in reference [16]. They can be applied to both major and minor nodes.

In the access area, switching will be accomplished by means of an access area switch. DCS plans indicate a DAX for this purpose. It will require timing for its functions and will be required to transmit timing to secure voice terminals homed on it. The candidate solutions for achieving a viable backbone timing subsystem extend to the access nodes. In reference [15, 16] alternatives are also discussed.

b. Communications Security Equipment. Dynamic stability is affected by communications security equipment in a synchronization (sync) sense. More specifically, the interaction of the key generators and multiplexers in a loss of sync phase, and any resulting destabilizing effects, must be determined.

(1) Reference Circuit. A simple reference circuit extending from the user, through switching, and to the radio in the transmission subsystem is considered in Figure 7-8. The two-level multiplex hierarchy common to DRAMA is shown as is the third-level multiplex as part of the digital radio subsystem.

(2) Synchronization Model. Models for frame synchronization, advanced by Kozuka [50], Sekimoto [51], and Benowitz, et. al. [52], have been studied to gain insight to the frame resync problem in terms of a Markov analysis. These models have considered a 193 bit frame. The specific Markov analysis corresponding to the mentioned models is given in reference [53]. The results, shown in Figure 7-9, demonstrate the validity of the Markov analysis. Benowitz's model was developed in more detail to determine the probability of a false match in 6 consecutive frame bits and the probability of false resynchronization. These results are given in Figure 7-10.

(3) Multiplex Hierarchy. When the analysis of the level 1 multiplex in Figure 7-8 was extended to the upper levels of the multiplex hierarchy, the number of states characterizing the Markov model quickly grew to the point where computer simulation was not feasible. This was true even assuming a simple framing strategy of 1 bit for both levels 2 and 3. The analysis was performed on a reduced scale to determine relative magnitudes of resynchronization times in terms of bit times.

From the preliminary results the model chosen for the three-level multiplex hierarchy is characterized by frame lengths of 3, 7 and 15 bits for the first, second and third levels, respectively. A channel error model [54] was used to develop the bit error statistics. It

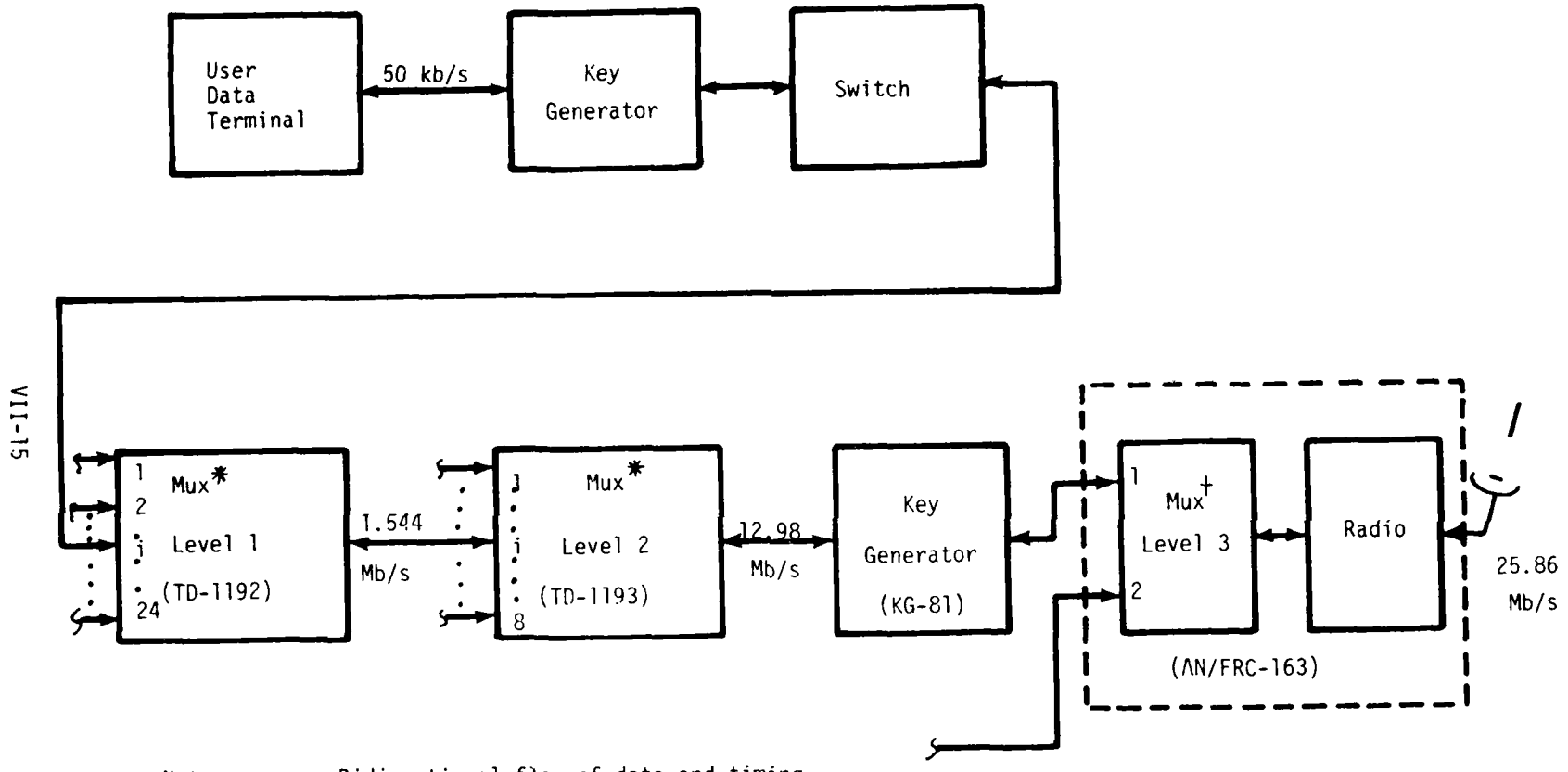


Figure 7-8. Typical Section of Reference Link for Initial Studies

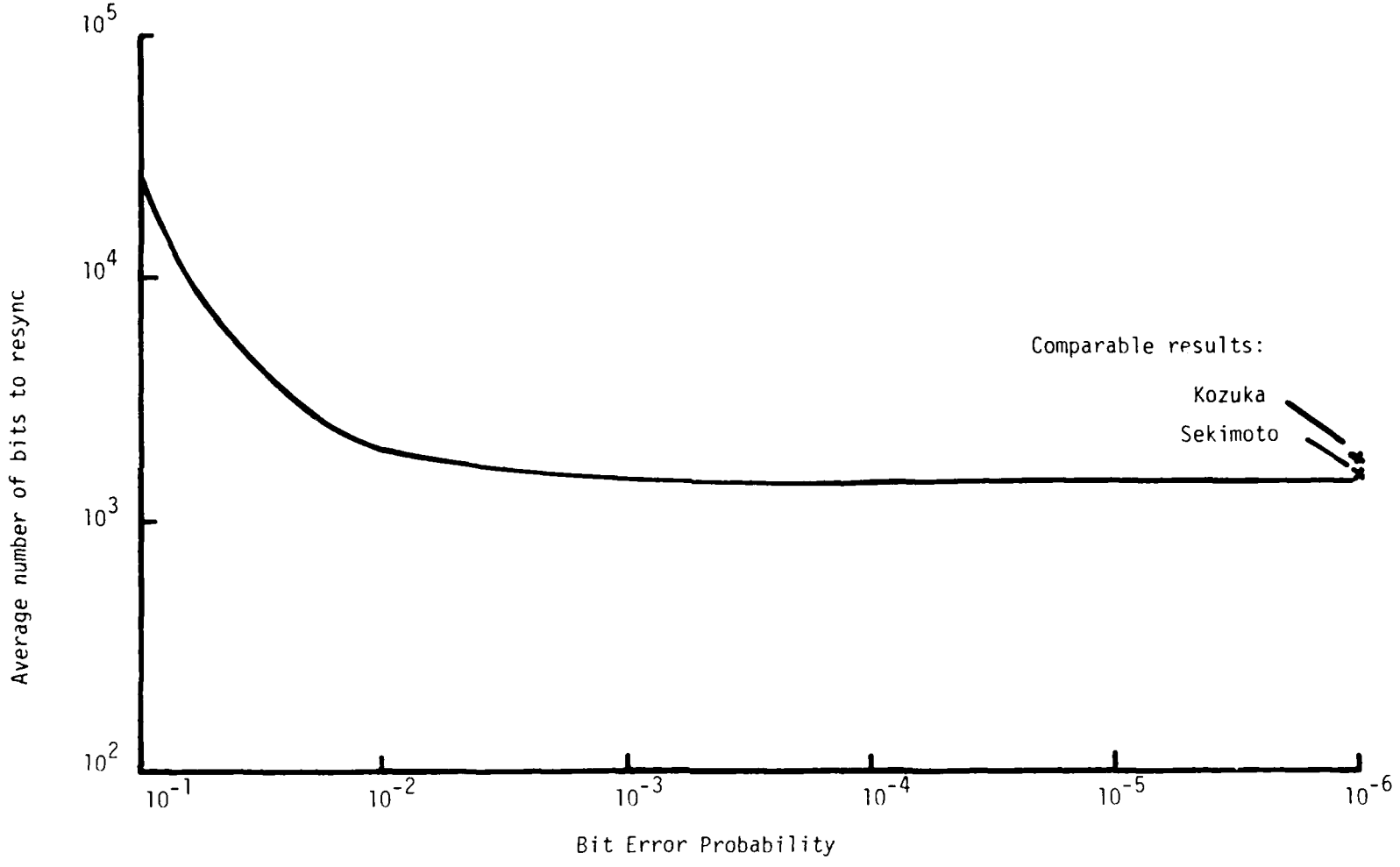


Figure 7-9. Expected Resync Time for AT&T DS-1 Frame

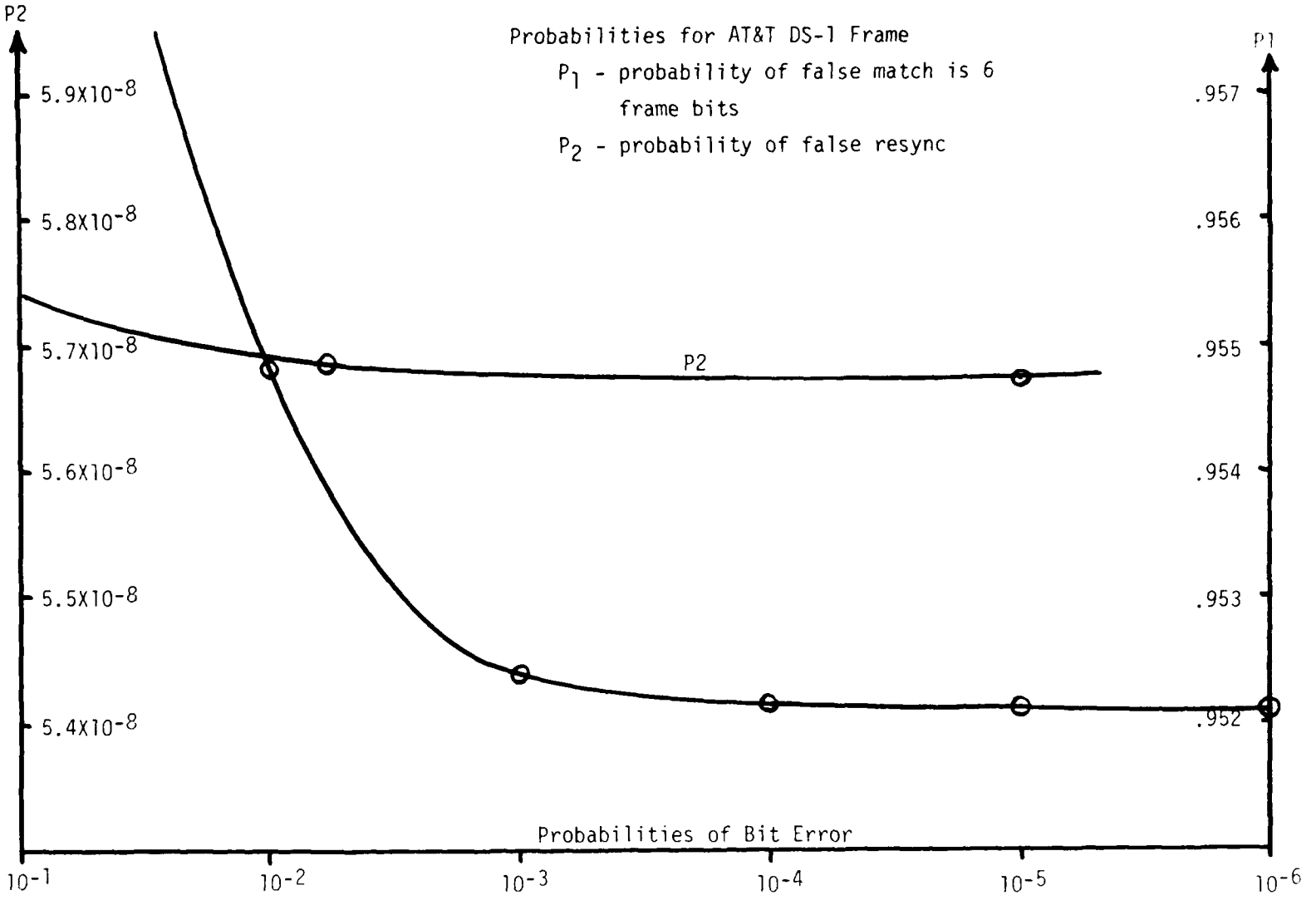


Figure 7-10. Probabilities for False Match and for False Resynchronization

was also assumed that if any level of the multiplex lost synchronism, so did all levels below it. Framing information is carried by a single bit in each of the three levels.

A Markov analysis was performed on this reduced model to determine reframe times as a function of bit slip probabilities at each of the three levels. The results are given in Tables 7-IV to 7-VI in terms of bits. Knowing the bit rates at the various levels of the multiplex therefore gives the times to reacquire synchronism.

c. Fault Propagation/Isolation. The dynamic stability of a communications network is an explicit function of the fault modes that can occur. Failure to stem the propagation of a fault can lead to system instability, as was previously indicated. The subsystems to be considered are identified, and failure modes and suggested actions are discussed.

(1) Reference Link. The reference link to be used was shown in Figure 7-8. It indicates the signal flows from a subscriber through a switch and transmission subsystems.

(2) Transmission. The transmission subsystem is assumed to be that described for the DRAMA program. Satellite transmission facilities will be factored into the reference circuit in future efforts, but are neglected now.

(3) Switching. A generic diagram of the switch is given in Figure 7-11. It is a functional block diagram for an all-digital circuit switch. The line formatter provides the interface with the full-duplex (4 wire) subscriber loops including loops to DAX's, concentrators and PBX's. The line formatter functions include: line termination, bit synchronization, line group multiplexing/demultiplexing, and detection of seize and release supervisory signals.

The trunk formatter provides the digital interface between the switch matrix and incoming and outgoing internodal trunk groups. The major functions of the trunk formatter are: trunk group termination, bit alignment, trunk group frame alignment, synchronization buffering to account for nodal clock differences, and extraction or insertion of signaling and supervision data into a common channel (common channel signaling, CCS, assumed).

The controller interface provides the controller with signaling and supervisory data from incoming lines and trunk groups, and generates such data via controller action for application to outgoing lines and trunk groups. The controller logic also provides the common logic for applying connection commands to the switch matrix.

TABLE 7-IV. MULTIPLEX RESYNCHRONIZATION AS A FUNCTION OF SLIP PROBABILITY AT FIRST LEVEL IN MUX HIERARCHY

	MUX LEVEL ASSUMPTIONS		
PROB. OF BIT SLIP AT LEVEL 1 PS_1	2, 3 in SYNC 1 OUT (BITS)	3 in SYNC 1 & 2 OUT (BITS)	1, 2 3 OUT OF SYNC (BITS)
0.00001	60.3	131.5	284.3
0.0001	60.6	131.6	284.2
0.001	63.6	133.4	283.6
0.01	93.2	151.6	280.5
0.1	75.5	215.7	307.8
0.5	60.5	131.9	495.4

$PS_2 = 10^{-5}$, $PS_3 = 10^{-3}$

TABLE 7-V. MULTIPLEX RESYNCHRONIZATION AS A FUNCTION OF SLIP PROBABILITY AT SECOND LEVEL IN MUX HIERARCHY

	MUX LEVEL ASSUMPTIONS		
PROB. OF BIT SLIP AT LEVEL 2 PS_2	2, 3 in SYNC 1 OUT (BITS)	3 in SYNC 1 & 2 OUT (BITS)	1, 2 3 OUT OF SYNC (BITS)
0.0001	60.3	131.4	284.2
0.001	60.3	131.5	284.3
0.01	60.6	132.6	284.8
0.1	63.6	143.4	290.0
0.5	90.8	175.3	309.4

$PS_1 = 10^{-5}$, $PS_3 = 10^{-3}$

TABLE 7-VI. MULTIPLEX RESYNCHRONIZATION AS A FUNCTION OF SLIP PROBABILITY AT THIRD LEVEL IN MUX HIERARCHY

	MUX LEVEL ASSUMPTIONS		
PROB. OF BIT SLIP AT LEVEL 3 PS_3	2, 3 in SYNC 1 OUT (BITS)	3 in SYNC 1 & 2 OUT (BITS)	1, 2 3 OUT OF SYNC (BITS)
0.0001	60.3	131.5	284.3
0.001	60.3	131.5	284.3
0.01	60.6	131.6	284.5
0.1	63.0	133.1	283.0
0.5	63.9	136.7	289.5

$PS_1 = 10^{-5}$, $PS_2 = 10^{-3}$

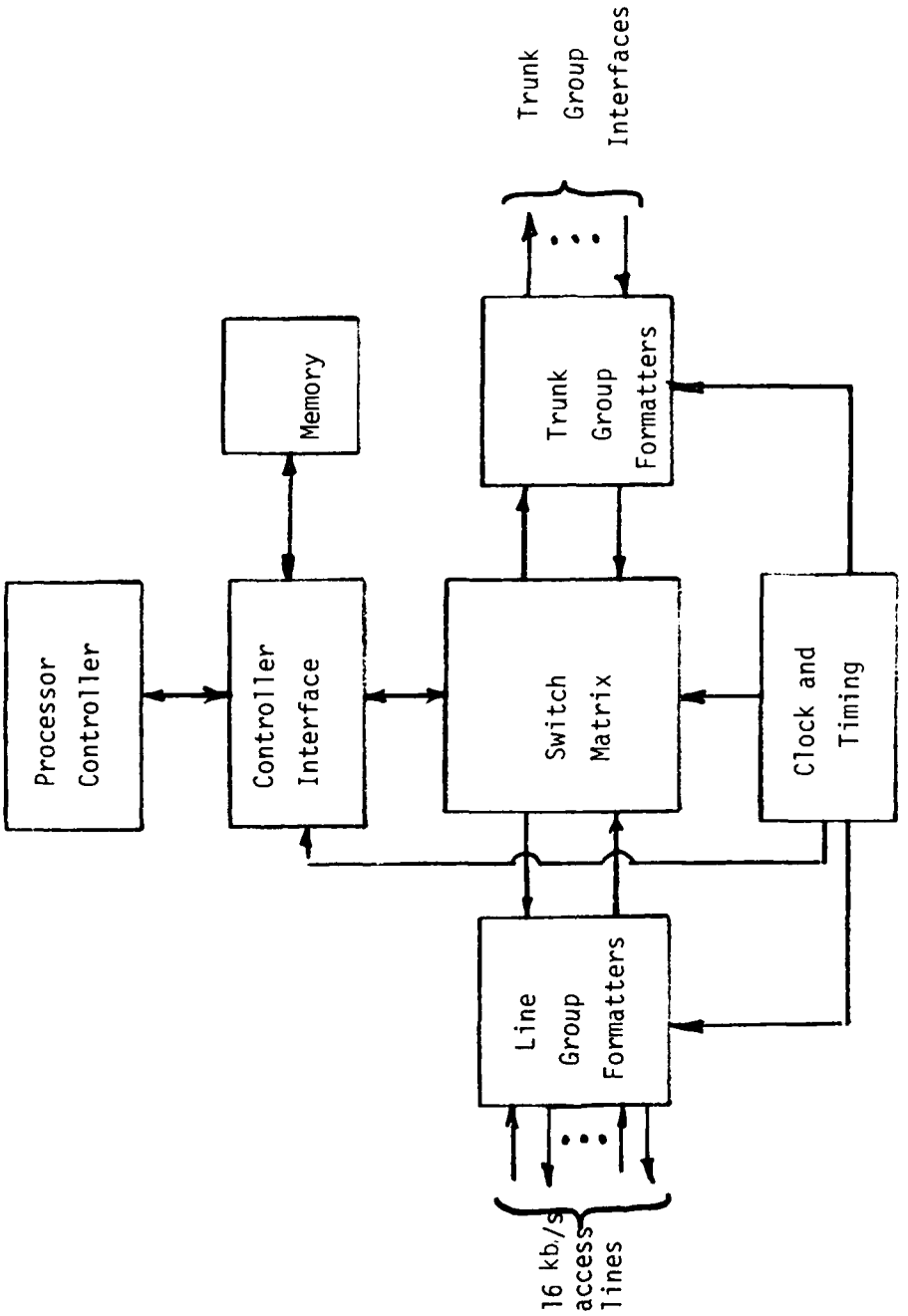


Figure 7-11. Time Division Switch Reference Model

The controller is a real-time, stored program processor designed for switching applications. The switch matrix accomplishes intra and inter-highway time slot interchange in response to connection commands received from the controller. The memory is provided for on-line programs, storage and tables including connectivity, routing, call progress and conference.

(4) User Subsystem. The DCS user population will utilize analog and digital voice and data in both clear and secure modes. The clear analog subscribers can access the digital system by either a PBX or a 4-wire connection. Clear data can achieve access through a modem/equalizer arrangement. Encrypted voice will access through an access area switch, probably a DAX, or a PBX in an enclave environment, or be bulk encrypted. Secure data will access the system in the form of encrypted, modemed signals and can be digitized by existing A/D techniques. Figure 7-12 shows the user location and interfaces are identified.

(5) Control. As mentioned, the control system can be divided into two parts, maintenance and operational direction. The function of the maintenance element is to restore the degraded subsystem element's service to normal levels. Status information consisting of alarm indications with outages and degradation reports is used to initiate appropriate maintenance responses. The frequency and timeliness of the status information depends, to a large extent, on the corresponding response time of the maintenance element which may be categorized as immediate responses (e.g., by technical controllers) or delayed responses (e.g., actions resulting from reports generated at a DCS nodal point).

Operational direction has the responsibility to ensure timely system responsiveness to the requirements of the DCS authorized users. The mission of operational direction includes the implementation of contingency plans and the optimization of the availability of communications resources for the use of approved critical users. Operational direction involves network reconfiguration, circuit allocations, reallocations, restoral and denials. These are carried out by exercising direction over various subordinate operational elements such as technical control facilities and switching centers, by alerting appropriate maintenance elements, or possibly by exercising direct control of system elements. Operational direction utilizes information related to major nodal equipment status, nodal configuration and data base, network traffic status, and network performance. This information provides the forcing function for initiating response control and direction over network operations.

d. Failure Mode Identification. For the subsystems indicated certain failure modes are identified. A subsequent section will consider the impact of these modes on the defined subsystems.

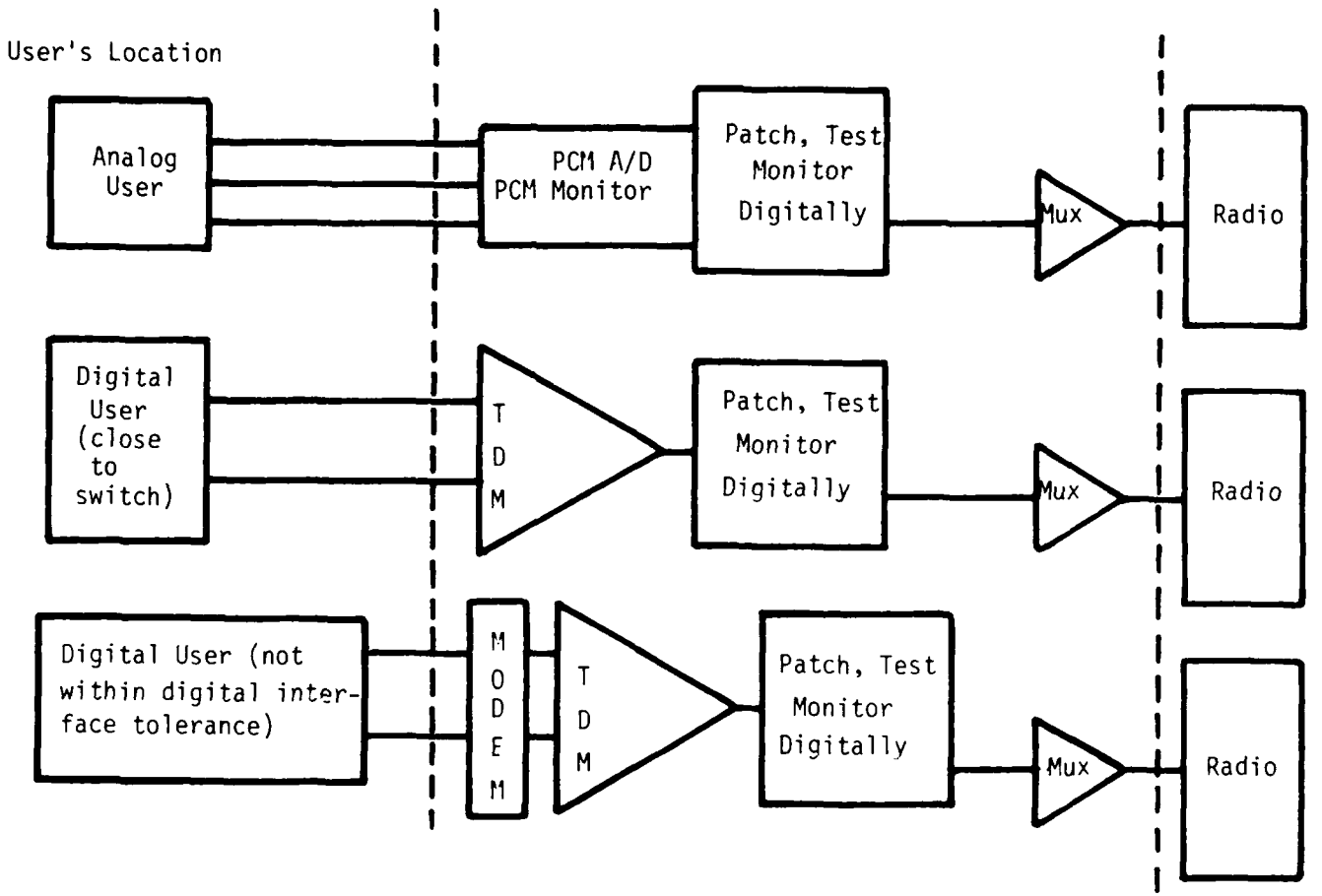


Figure 7-12. User Location and Interface Model

(1) Transmission. The failure modes include:

- Loss of timing and sync (including any interruption)
- Loss of multiplex function (any levels)
- Loss of crypto, and crypto imbedding
- Loss of digital radio

(2) Switching. As shown in Figure 7-11, several important blocks exist. For example, the switch matrix or the processor controller have binary failure modes; they do not appear to fail softly. The switch cannot operate without these functions. Other failure modes include:

- Memory failure - inability to access memory
- Controller interface
- Line and trunk formatters - including their subfunction
- Clock and timing failure - degraded, and total failed status
- Processor controller and switch matrix - as mentioned

(3) User (Subscriber). Clear voice and data analog access area subscribers do not appear to have failure modes that have a major impact on other subsystems. They also will not be digitized at the end instrument. High speed data may be the only exception, since it already exists in digital form; but it will access the system through a modem. The failure modes occur for encrypted access traffic and pervade both voice and data. The modes include:

- Encryption device
- Modems

(4) Control System. The elements of the controller subsystem, as mentioned, are maintenance control and operational direction. The failure modes include:

- Tech control at the switch
- Maintenance control at switch node (but for transmission subsystem)
- Communication failures between operations centers

e. Fault Isolation Examples. If a fault in the system occurs, the first question to be asked is can the fault be immediately isolated? If not, the next question is what is the radius of propagation; that is, what effects will fault propagation have on other subsystems.

One of the key elements in any stability discussion is that of system timing. This element pervades not only transmission and switching, but also the user, if time must be transferred to his terminal. This element has been treated in an earlier section, with specific reference to stability, and is therefore not discussed further in this section.

(1) Synchronization. Consider that frame synchronization in the multiplex hierarchy on the receiver side of a node is faulted. The immediate result is a multiplex frame sync alarm. However, any encryption equipments receiving information from the affected multiplexer would be alarmed. This is not desired since the encryption device could be operating normally. If it is alarmed, a resynchronization of both the multiplexer and encryption device could result.

Consider that encryption equipment exists between a higher and a lower level multiplex, as shown in Figure 7-13. If the higher level multiplex (HLM) loses sync it is desirable to maintain the encryption device (KG) in operation until the multiplexer requires sync, or determines that it cannot resync. However, the KG is slaved to the multiplexers for sync information. Hence, to force the KG to continue operation in the event that frame sync loss occurs at the higher level may necessitate a control element between the HLM and the KB. If either the HLM or the KG loses sync, the lower level multiplex (LLM) is affected because it depends on correct decryption of the data stream for its sync code detection. Loss of sync at either the HLM or KG therefore destroys the sync information needed by the LLM. In addition, the LLM does not know if it is at fault or the sync loss occurred elsewhere. The control element appears to be the key to this problem.

When sync is lost at the HLM, the control element must inhibit both the KG and the LLM from initiating a sync search. If this is not accomplished, each of the multiplexers and the KG would automatically and independently initiate a resync procedure. This could result in a resync oscillation since the operation of both the KG and the LLM depends explicitly on the HLM being in sync. Operation of the LLM requires that the HLM and the KG be in sync. If the KG loses sync, but the HLM does not, the control element inhibits the LLM from initiating a sync search, since this multiplexer again detects its sync from the decrypted stream. Resynchronization therefore, is initiated by the KG, not by the LLM. Once crypto resync is established, given that the HLM is in sync and that the sync information required by the LLM has not been corrupted in the transmission medium, the LLM should be immediately in sync requiring no resync procedure. Figure 7-14 shows a flow diagram of frame or crypto synchronism loss in the transmission subsystem or the receive side of a node.

Similar reasoning would hold for replacing the encryption choice with a multiplexer in a hierarchical arrangement, except that control functions would be exercised by the multiplexers rather than through a discrete control element. This control would then inhibit automatic resynchronization procedures in the lower levels of the multiplex hierarchy should a sync fault occur in a higher level. Once the resynchronization is accomplished at the higher level, all lower level multiplexers should be immediately synchronized, and therefore,

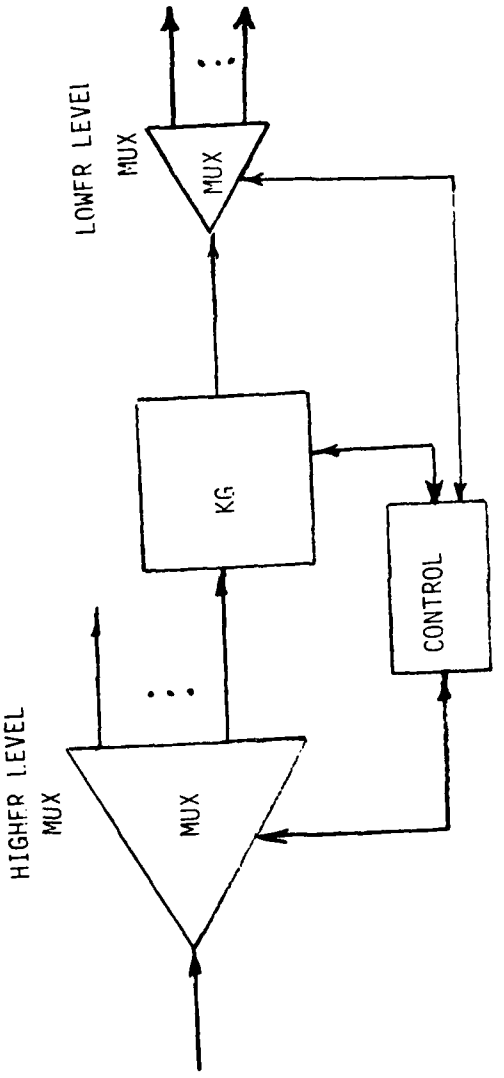


Figure 7-13. Two-Level Multiplex Hierarchy With Control Element

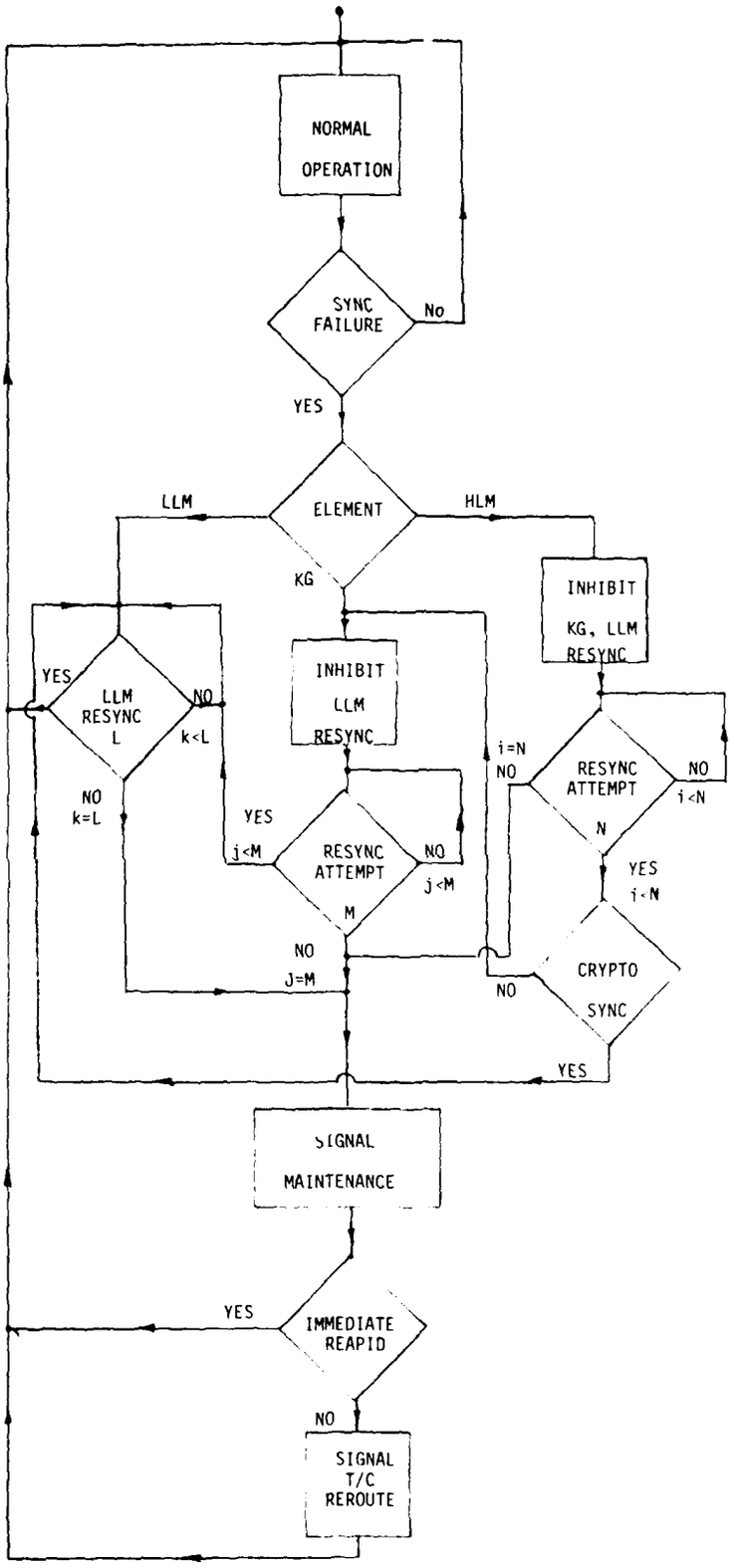


Figure 7-14. Flow Diagram - Transmission Resynchronization (Receive Mode)

do not have to initiate their own independent resync procedures. This results, as in the previous discussions, because once the higher level multiplex has reacquired sync, it performs the correct demultiplexing function resulting in correctly framed data streams to be input to the lower levels of the hierarchy. This presumes the sync information governing the lower levels has not been corrupted in the transmission medium.

To this point, discussions have centered on the receiver side of the transmission subsystem. Again consider Figure 7-13, but now in a transmit mode. If the LLM faults, neither the KG nor the HLM operation is affected since their operation is independent of that of the LLM. What could occur is that the control element could sense the LLM failure, inhibit the KG output to the HLM, and maintain the KG in operation. The HLM would operate normally. If the KG lost sync, the HLM operation would be unaffected. The KG would be inhibited from accepting the LLM output. However, it would not be desirable to inhibit LLM operation since the KG fault would then spread to the LLM. The LLM would in essence accept its inputs, in a normal fashion, and discard the multiplexed output destined for the affected KG until it reacquired sync. If the HLM loses sync, the operation of the KG and LLM remains unaffected. However, the output of the KG is discarded until the HLM reacquires sync. In this manner then, the transmit elements can be made essentially independent in operation. Figure 7-15 shows the corresponding flow diagram.

In the previous discussions it has been assumed the KG can resync using the received data stream only, and that no other KG resynchronization procedure need be effected. This assumption is true if the KG operates in a key-auto-key (KAK) mode. However, if it operates in a mode such as Cipher-text-auto-key (CTAK) it cannot resync using the data stream information only. In such a case, the KG must effect resynchronization by communicating with its mate, since key generators are paired, at the other end of the transmission pipe. Operating in such a mode, therefore, necessitates a crypto pair resync if either the KG or the HLM loses sync. The KG would remain unaffected if the LLM lost sync.

In the examples considered for frame and crypto sync loss, the switch need not know that a sync loss occurred unless the resync operation fails. This is also true for other equipment failure modes. Such failures necessitate maintenance intervention, and the switch must be prohibited from assigning traffic to the affected equipments. If maintenance cannot be effected within a specific time, a signal must be passed to the technical control element to institute a rerouting procedure in the switch. This signal would not identify which equipment faulted, but would indicate that rerouting of affected traffic is necessary. This rerouting impacts dynamic stability because it introduces transients which can affect switching in terms of blocking and congestion, or transmission in terms of capacity. This particular topic will be the subject of future work.

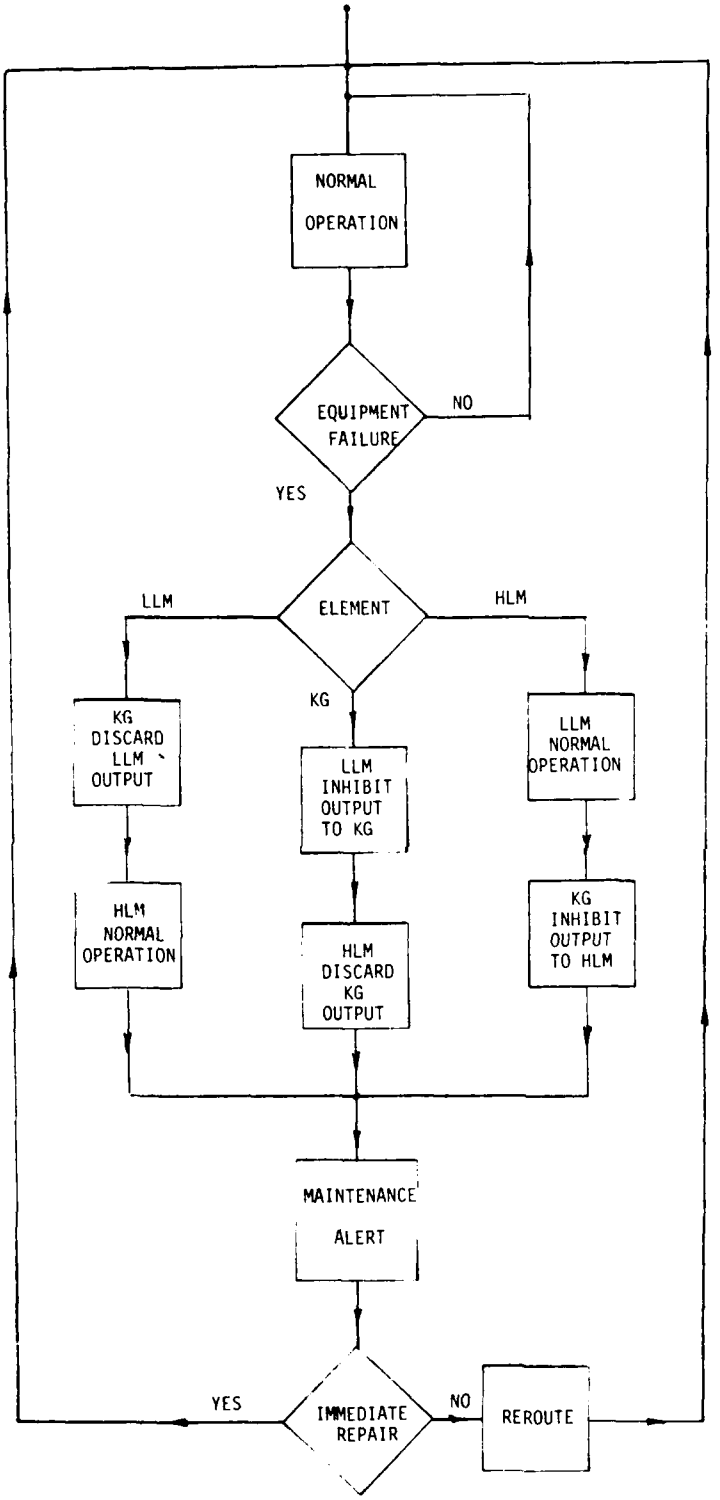


Figure 7-15. Flow Diagram - Equipment Failure of Transmission Subsystem (Send Mode)

(2) Maintenance Activity. The loss of frame and acquisition failure, or an equipment malfunction, can cause unnecessary maintenance and technical control activities at both ends of the affected transmission path. For example, consider that the transmission medium experiences a short, temporary outage. Alarms are sounded at both ends of the affected transmission path, indicating a fault exists. The problem is then one of fault isolation. However, the cause of the fault may not be immediately known. A seriously degraded signal level, for example, might be caused either by the transmission media or by a transmit radio failure. The symptoms could be identical. Rerouting affected circuits offers a solution. However, circuit rerouting introduces an unwanted transient into the system, thereby impacting system stability In addition, the fault may be cleared by the time rerouting has been completed. Hence, the maintenance activity and technical control rerouting would be unnecessary. This is true for temporary outages resulting from fading transmission media. It is not true for permanent outages.

As another example of the impact of maintenance activity on system stability, consider that the transmission medium is degrading the transmitted signal. This degradation may be only slightly below tolerance thresholds; however it results in an increased bit error rate environment but not loss of communication, as in the previous example. Alarms are sounded indicating signal degradation with possible loss of sync. The problem now becomes one of determining if the affected channels should be logged out-of-service and the affected traffic rerouted while testing is initiated. If the degradation persists, such activity is necessary. If the degradation does not, such activity could propagate the fault condition.

The point to be stressed in these maintenance activity examples is that a temporary fault can cause unnecessary activity and result in a propagation of the fault. The impact of this activity is not yet known, but is the subject of studies presently being conducted.

(3) Encryption Imbedding. One important aspect of dynamic stability is the propagation of faults, which results in undesired oscillations in the system. Examples of these oscillations were presented in the discussion of synchronization loss in a multiplex hierarchy containing COMSEC equipment. An important example to be discussed here is that of COMSEC equipment imbedding, specifically that of properly operating encryption equipments becoming affected by faults in either the transmission or switching subsystems.

Figure 7-16 shows an example of encryption imbedding wherein the transmission subsystem KG's, required for traffic security between nodes, are imbedded in a path terminated by DSVT's. The KG pairs are indicated in the figure. Any disruption in communications between any two paired KG's will not cause other paired KG's to be affected This results

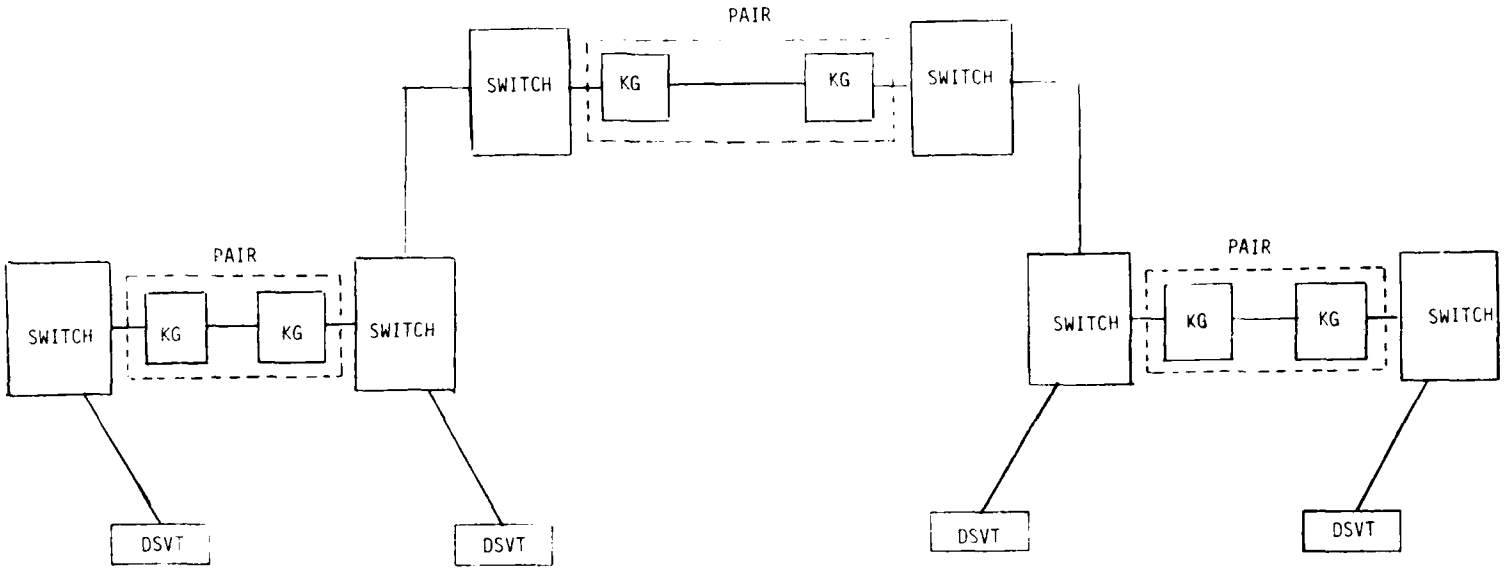


Figure 7-16. Encryption Imbedding - Crypto Pairs

because there is no communication between inter-paired KG's. That is, each pair is isolated from all other pairs by major switching nodes. The pairs are not imbedded.

The DSVT pair, however, will be affected by communications disruption anywhere in the path. They can only resync after the disruption has been cleared. Hence, the occurrence of a fault between a KG pair, while isolated, necessarily propagates to affect DSVT crypto synchronism Occurrence of a fault at either the DSVT or in transmission between the DSVT and the switch to which it is homed will not cause a fault propagation to any KG pairs.

Also of interest is an example in which DCS subscribers have their own encryption device (not DSVT's), and are brought into the network at a minor node through drop and insert capabilities. Figure 7-17 illustrates this idea. The minor node subscribers have imbedded encryption devices because the KG pair is located between nodes. If the KG pair loses sync, communications are disrupted between the special subscribers. This can necessitate resynchroniztion of the special subscribers encryption devices. Hence, as in the previous example, a loss of communications between paired KG's can result in this fault being necessarily propagated to the subscriber level.

4. DISCUSSION

The problem of dynamic communications stability has been developed by means of examples which have treated timing buffer stability, synchronization, maintenance activity and encryption imbedding. Fault modes were identified in relation to the examples and the effects of fault propagation were discussed.

It has been found that for frame synchronization loss, a control element could aid in the minimization of sync loss propagation to various levels in the hierarchy, including COMSEC equipments. Unnecessary maintenance activity, causing transients in the system, could result from switch or transmission faults. The result would be a spreading of the fault. Encryption imbedding can cause a fault propagation that is unavoidable.

Studies are presently being conducted to determine analytically the net effect of fault propagation on system performance, the character of the oscillations set up by failure mode propagations, and the system response.

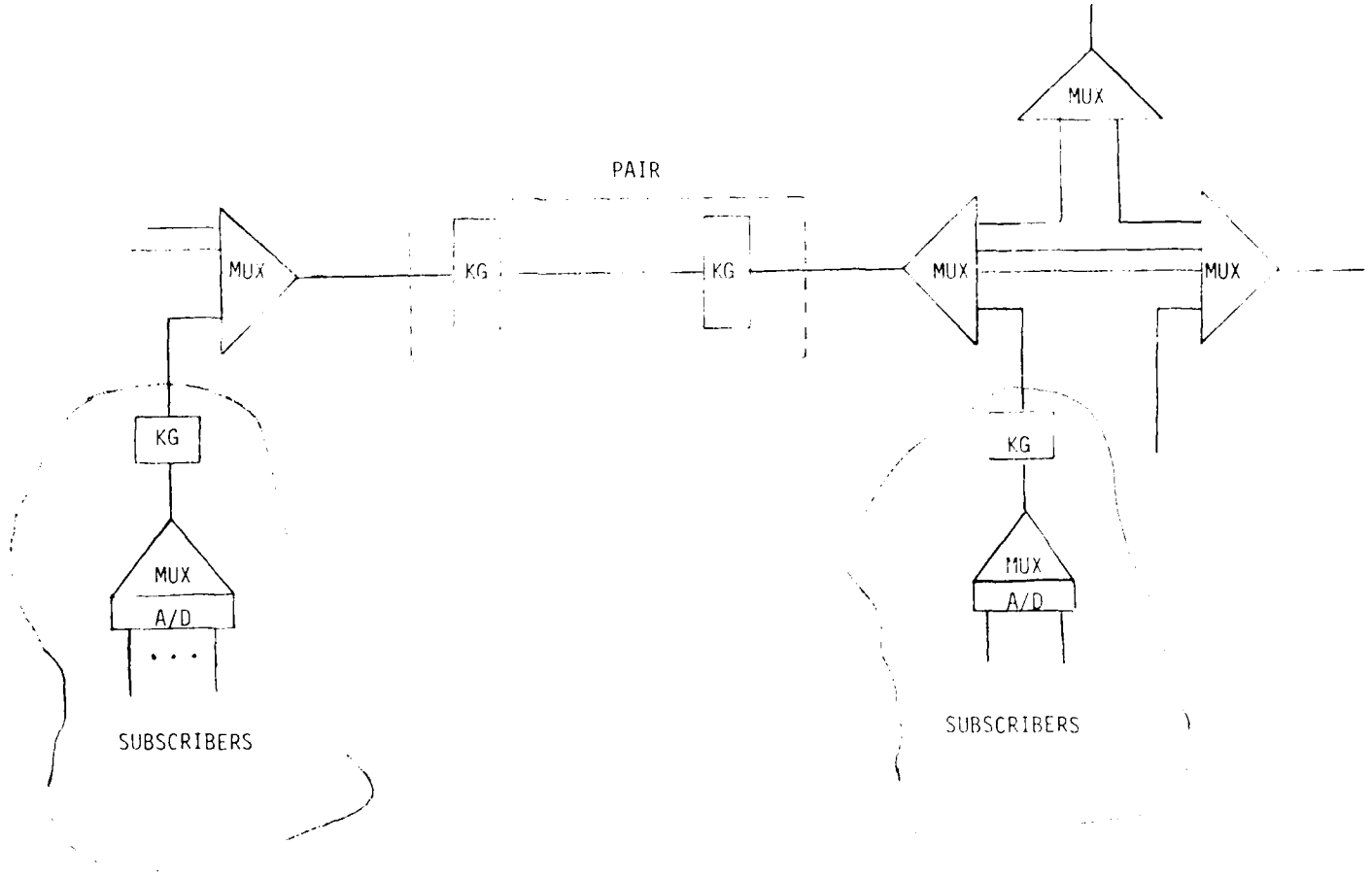


Figure 7-17. Encryption Imbedding - Special Subscribers

VIII. SUMMARY CONCLUSIONS

1. GENERAL

Six system-level issues have been defined, described, discussed, and analyzed. These issues do not represent the full range of issues which will require resolution during the process of moving toward DCS II; however, this effort represents another step in interfacing and integrating the various subsystems and elements. The issues addressed in this report are those perceived as most critical at the present stage of DCS evolution.

As the programs and projects associated with DCS II advance into the implementation phase, then on to operational status, it is inevitable that additional technical details will become known thereby surfacing a greater number of issues for resolution.

2. SUBSYSTEM INTERFACES - INFORMATION EXCHANGE AMONG MAJOR DCS SUBSYSTEMS AND ELEMENTS

The information needs of major DCS subsystems and elements have been identified and tabulated via 13 information exchange tables. Specific examples are presented; however, the tabulation is not intended to be complete or exhaustive. The tables demonstrate the type of information interchange that should be considered for near-term project implementation as well as long-term program objectives. The following future actions are required:

- Detailed review of the information tables and data flow by headquarters DCA and the appropriate engineering offices of the military departments.
- Initiate a specification control process to ensure that future DCS subsystems and elements exchange information as conceptualized.
- Propose specification changes to the hardware and software for on-going developments or procurements, particularly with respect to DRAMA, AN/TTC-39, DAX and SYSCON.

3. AUTOSEVOCOM II/DIGITAL TRANSMISSION INTERFACE

This analysis considered three basic concepts from which 13 variations of alternatives for interfacing the AN/TTC-39 and DRAMA were evaluated. The results indicate that the alternatives

addressed under Concept II (i.e., alternative 1b or 2b) would be the prudent near-term course of action for DCA, considering the very real possibility of implementing the Digital European Backbone, Phases I-IV, by the early 1980's. Alternatives 1b and 2b are manual in nature, similar to the present arrangement in AUTOVON. On the basis of cost, coupled with schedule risk, alternative 1b appears more attractive.

For the far-term, depending on the growth of AUTOSEVOCOM II traffic, Concept I and Concept III (i.e., automation of technical control functions) should be analyzed further.

4. TRANSMISSION DIGITIZATION STRATEGY - PCM VS DM

Although the present implementation plans for DEB call for the utilization of 64 kb/s PCM for general voice channel use, certain advantages and disadvantages of delta modulation necessitated an evaluation of these two possible strategies. The results of the study indicate that the advantages of a "PCM only" strategy outweigh the advantages of a combined PCM/DM strategy for the near-term (i.e., DEB implementation). See the calculated figure of merit. For the far-term, the potential increase in channel capacity using a combined PCM/DM strategy justifies further consideration.

5. DCS ENCRYPTION

This analysis examined three alternative strategies for DCS encryption: (1) end-to-end encryption, (2) bulk encryption from secure enclaves, and (3) PBX-to-PBX encryption from secure enclaves. The idea of enclaves was advanced as a plausible solution to certain subscriber encryption requirements.

The results indicate that alternatives (1) and (3) are attractive courses of action and should be considered for application during the evolution of AUTOSEVOCOM II.

It is anticipated that DCA and NSA jointly will develop a program for further consideration of the two courses of action.

6. SOFTWARE COST MINIMIZATION

Software cost is an area with enormous potential for cost growths that must be brought under control. This study analyzes historical data on major DoD system acquisition programs which experienced large expenditures in software.

On the basis of the analysis, various courses of action, both in-house and contractual efforts, are being considered.

7. DYNAMIC STABILITY

Dynamic stability is a characteristic of any large switched communications system. It can be thought of as the resistance of the system to unstable oscillations brought about by conceivable failure modes. Dynamic stability within the DCS was explored by means of examples which considered timing buffer stability, synchronization, maintenance activity and encryption imbedding. Fault modes were identified in relation to the examples, and the effects of fault propagation were discussed.

It has been found that (1) a control element could aid in minimizing the effects of fault propagation within the multiplex hierarchy, (2) switch or transmission faults causing transients throughout the system may result in unnecessary maintenance activity and further propagation of the fault, and (3) encryption imbedding can cause a fault propagation that is unavoidable.

Studies now in progress to determine the net effect of fault propagation on system performance will be continued. These studies will be analytical as well as specific equipment oriented.

IX. REFERENCES AND BIBLIOGRAPHY

REFERENCES

[1] System Control Inc. Report, "Hierarchy/Configuration Architecture Study for the System Control Subsystem of the Future DCS." Sep 1976.

[2] DCEC TR 12-76, "DCS Digital Transmission System Performance," Appendix A, May 1976.

[3] Preliminary TR 29-76,"Preliminary DCS/Voice Network Design," Sep 1976.

[4] TRI-TAC Spec. No. TT-B1-1101-0001A, "Performance Specification Control Office, Communications, Automatic AN/TTC-39 ( ) (V)," 7 Jun 1976.

[5] DCEC Internal Memorandum (Draft),"AUTOSEVOCOM/Digital Transmission Interface," M. Fluk.

[6] TRI-TAC Spec. No. TTD1-3002-0012, "Performance Specification Communications Nodal Control Element (CNCE)." 6 Dec 1974.

[7] ESD Working Paper,"Data Adapter and TCCF Life Cycle Costs," Dec 1974.

[8] DCEC TR 3-74, "Digital Transmission System Design," Mar 1974.

[9] DCA Paper, "Introduction of TDM into the DCS," 2 Jan 1969.

[10] DCEC TR 20-75, "Engineering Concepts for DCS Transition," July 1975 (SECRET).

[11] DCEC Internal Memorandum, "Evolutionary Approaches for Backbone Transmission and Digitization," LCDR A.K. Perry, June 1976.

[12] DCEC TR 1-77, "Planning and Programming Transition Issues," Apr 1977.

[13] DCEC Spec. (Draft), "Digital Transmission System Specification."

[14] TRI-TAC Spec. No. TT-A3-9009-0041, "Rekeying Plan for Digital Circuit Switches and Associated Equipment," 24 Sep 76.

[15] DCEC TN 27-76, "A Timing and Synchronization For The Access Area," R.H. Bittel, Oct 1976.

[16] DCEC TN 43-75, "Communications Network Timing," H.A. Stover, Sep 1975.

[17] DCEC Report (Draft), "Functional Description Digital Access Exchange," 15 Oct 1976.

[18] DCEC TN 25-76, "Technical Feasibility of PBX-to-PBX Security," R.H. Bittel, Oct 1976 (Confidential).

[19] USAF Project Rand Report,"Air Force Command and Control Information Processing in the 1980's: Trends in Software Technology," Donald W. Kosy, Jun 1974.

[20] Robert C. Chen, Perter G. Jessel, and Robert A. Patterson, "Mininet: A Microprocessor-Controlled Mininetwork," Proc. IEEE, 64, No. 6, (Jun 1976).

[21] GTE Automatic Electric Laboratories, Internal Document, "Management of Software Development," Edmund B. Daly, 1976.

[22] Ellis Horowitz (ed.), Practical Strategies for Developing Large Software Systems, Addison-Wesley (1976).

[23] A. Kossiahoff, T.P. Sleight, E.C. Prettyan, J.M. Park, and P.L. Hazan, DoD Weapon Systems Software Management Study, Jun 1975.

[24] Jack Goldberg (ed.), Proceedings of a Symposium on the High Cost of Software, Stanford Research Institute, Menlo Park, CA.

[25] David S. Alberts, "The Economics of Software Quality Assurance," AFIPS Conf. Proc. 45, 1976.

[26] Robert Bruno, Personal Interview, Air Products and Chemicals Corporate Headquarters, Management Information Department, Trexlertown, Pa., 1974.

[27] B.W. Boehm, et al., "Characteristics of Software Quality," TRW Software Series (Dec 1973).

[28] DoD TIN Man Report, "Requirements for High Order Language," Lt Col William A. Whitaker (ed.), Jun 1976.

[29] Donald I. Good, "Provable Programming," Proc. International Conf. on Reliable Software (Apr 1975).

[30] Donald J. Reifer, "Software Specification Techniques: A Tutorial," Proc. 13th IEEE Computer Soc. Int. Conf. (Sep 7-10, 1976) pp 29-43.

[31] H.M. Broneman, and L. Danielman, "Software Design for Hardware Interaction on Real-Time Military Systems," Proc. 13th IEEE Computer Soc. Int. Conf., Hughes Aircraft Company, Culver City, CA. (1976) pp 89-101.

[32] E.W. Dijkstra, "The Structure of the "THE" - Multi Programming System," Communications AGM, 11, No. 5, (Sep 1969) p 489.

[33] Harry Katzan, Jr., Systems Design and Documentation - An Introduction to the HIPO Method, Van Nostrand Reinhold Co. (1976).

[34] Peter Freeman, "Toward Improved Review of Software Design," Proc. National Computer Conf. 44, AFIPS Press (1975) pp 329-334.

[35] Peter G. Neumann, "Software Development & Proofs of Multi-Level Security," Second Int. Conf. on Software Eng., San Francisco, CA (Oct 1976) pp 13-15.

[36] D.L. Parnas, "On the Criteria to be Used in Decomposing Systems into Modules," Com. of the ACM, 15, No. 12, (Dec 1972) pp 1053-1058.

[37] D.L. Parnas, "On the Design and Development of Program Families," IEEE Trans Software Eng., SE-2, No. 1, (Mar 1976) pp 1-8.

[38] L. Pouzin, Infotech State of the Art Report 24, "Network Protocols - Network Systems and Software," (1975) pp 601-627.

[39] Ray W. Sanders and Vinton G. Cerf, "Compatibility of Chaos in Communications," Datamation (March 1976).

[40] RADC Report No. RADC-TR-69-190, "Communications Computer Language COMTRAN," David W. Clark, July 1969.

[41] W.A. Wulf, Ralph L. London, and Mary Shaw, Abstraction & Verification in ALPHARD: Introduction to Language and Methodology, Department of Computer Science, Carnegie-Mellon University, Jun 1976.

[42] Clement L. McGowan and John R. Kelley, Top Down Structured Programming Techniques, Pertocelli/Charter, New York (1975).

[43] S.L. Gerhart and L. Yelowitz, "Observations of Fallibility in Applications of Modern Programming Methodologies," IEEE Trans. Software Eng. SE-2, No. 3,(Sep 1976).

[44] William E. Carlson, (coordinator), "Improving Dod Software Engineering Capabilities - The DARPA Approach," a report prepared by the Defense Advanced Research Projects Agency (DARPA) in coordination with the Research and Development Coordinating Panel of Management Steering Committee for Embedded Computer Resources, June 1976.

[45] Terry F. Baker, "Structured Programming in a Production Programming Environment," IEEE Trans. Software Eng. SE-1, No. 2, (June 1975) p 241.

[46] H. Bratman and T. Court, "The Software Factory," Computer, (May 1975) p 28.

[47] DCEC TN 24-73, "Programming Languages for Communicating Processors," P.M. Cohen, May 1973.

[48] DCEC TR 12-76, "DCS Digital Transmission System Performance," K. Kirk, Nov 1976.

[49] DCEC Technical Note, (To be published), "DCS Interim Timing," Dave Smith

[50] S. Kozuka, "Transmission Characteristics of Pulse Stuffing Synchronization System," Rev. Elec. Comm. Lab., 18, No. 5-6,(May-June 1970) pp 296-305.

[51] T. Sekimoto and H. Kaneko, "Group Synchronization for Digital Transmission Systems," IRE Trans. Comm. Sys. (Dec 1962) pp 381-390.

[52] P. Benowitz, et al., "Digital Multiplexers," BSTJ, 54, No. 5,(May-June 1975) pp 813-919.

[53] Progress Notes, Contract RADC No. F30602-75-C-0118, "Development of a Dynamic Stability Model for a Digital DCS," J. Hammond and S.S. Liu, Jul 15, 1976.

[54] K. Brayer, Data Communication Via Fading Channels, IEEE Press (1975).

BIBLIOGRAPHY

1. DCA Study, "DCA Operations Management Information System 1974-1978 (Draft)," 10 Apr 1974.

2. DCEC TN 5-75, "A System Control Alternative Analysis," Apr 1975.

3. DCEC TR 5-74, "DCS System Control Concept Formulation," Feb 1974.

4. DCA Spec., "System Performance Specification for AUTODIN II Phase I," Nov 1975.

5. Spec. No. DCEC-220 (Draft), "Digital Transmission System Specification," Sep 1976.

6. Spec. No. TTC-A3-9004-0019, "Interface Specification of the TCCF and AN/TTC-39," Dec 1974.

7. Computer Science Corp., Report No. RADC-TR-75-42, "Integrated Switching/Multiplexing/Tech Control," Mar 1975.

8. Stanford Telecommunications, Inc., "Definition of Real-Time Adaptive Control (RTAC) for the Defense Satellite Communications System (DSCS)," (to be published Nov 1976).

9. GTE Sylvania, Inc. Report, Contract No. DCA-100-76-0041, "Augumented Autovon Switch Study," 1 & 2, 9 Sep 1976.

10. USACEIA Spec No. CCC-74047, "Specification for PCM Multiplex Terminal (1st level MUX)," 11 Feb 1975.

11. USACEIA Spec. No. CCC-74048, "Specification for Multiplexer/ Demultiplexer TD-1193," Feb 1975.

12. Martin-Marietta Internal Spec., Specification No. HPS 90600000-002, "CRF and ADT Hardware," Undated.

13. DCEC TR 12-76, "DCS Digital Transmission System Performance," May 1976, Appendix A.

14. "Code Modulation with Digitally Controlled Companding for Speech Transmission," Phillips Technical Review, 31, No. 11/12 (1970).

15. N.S. Jayant, K. Shipley, "Multiple Delta Modulation of a Speech Signal," Proc. IEEE, (Sep 1971).

16 Harris Corp. Internal Memorandum "CVSD Performance with Quasi Analog Signals," N.C. Seiler, 30 Jan 1976.

17. H.R. Schindler, "Delta Modulation" IEEE Spectrum (Oct 1970).

18. Schwartz, Bennett, Stein, Communication Systems and Techniques, McGraw-Hill, 1966.

19. DCEC TN 24-76, "Requirements and Constraints For The Design Of The DCS Voice Network," Scharf and G. Kelley, Aug 1976 (Confidential).

20. DCEC TN 4-77, "COMSEC Optimization," Grace Kelleher, (To be published).

21. Charlie Bass and Dean Brown, "A Perspective on Microcomputer Software," Proc. IEEE, 64, No. 6 (Jun 1976).

22. Richard H. Bigelow, Norton R. Greenfield, Peter Szolovit and Frederick B. Thompson, "Specialized Languages: An Applications Methodology," AFIPS Conf. Proc. 42, (1973) pp M49-M53.

23. B.W. Boehm, et al., "Some Experience with Automated Aids to the Design of Large-Scale Reliable Software," IEEE Trans. Software Eng. TRW, (Mar 1976).

24. Bolt Beranck and Newman, Inc., Report No. 3261, "Development of a Communications Oriented Language, Parts I & II," Mar 1976.

25. Robert F. Bridge, Edward W. Thompson, The University of Texas at Austin, Electronics Research Center, Technical Report No. 163, "A Module Interface Specification Language," Dec 3, 1974.

26. J.M. Buxton and B. Randell (eds.), "Software Engineering Techniques," Scientific Affairs Division, NATO, Brussels, Apr 1970.

27. Yaohan Chu and E. Raymond Cannon, "Interactive High-Level Language Direct-Execution Microprocessor System," IEEE Trans. Software Eng. SE-2, No. 2 (June 1976).

BIBLIOGRAPHY (CONTINUED)

28. L.M. Culpepper, "A System for Reliable Engineering Software," IEEE Trans. Software Eng., SE-1, No. 2 (Jun 1975), p 174.

29. J.W. Cuthbert, "A System for Procuring and Controlling Modular Computer Programs," 18th Annual Meeting, Engineering Data Management and Computer Aided Design Technology sections of the American Defense Preparedness Association, May 5-7, 1976.

30. J.B. Dennis and E.C. Van Horn, "Programming Semantics for Multi-programmed Computations," Communications ACM, 9, No. 3.

31. Department of the Army Technical Bulletin, "Management Information Systems Handbook of ADP Resource Estimating Procedures (ADPREP)," Jul 1975.

32. F. DeRemer and H.H. Korn, "Programming in the Large Versus Programming in the Small," IEEE Trans. Software Eng. SE-2, No. 2 (June 1976).

33. E.W. Dijkstra, F. Genuys (ed.) "Co-operating Sequential Processes," Programming Lanuages, Academic Press, 196[illegible].

34. Bernard Elspas, Karl N. Levitt, Richard J. Waldinger and Abraham Waksman, "An Assessment of Techniques for Proving Program Correctness," ACM Computing Surveys, 4, No. [illegible] (June 1972).

35. Institude for Defense Analyses Paper, "Automatic Data Processing Costs in the Defense Department," David [illegible] (Oct 1974) p 1046.

36. J.B. Gerhart (Coordinator), "Software Development and Configuration Management Manual," TRW Software Series, Dec 1973.

37. Jim Gibbons, "When To Use Higher-Level Languages In Microcomputer-Based Systems," Electronics (Aug 7, 1975).

38. J.A. Gosden, "Explicit Parallel Processing Description and Control in Programs for Multi- and Uni-Processor Computers," AFIPS Conf. Proc. Fall Joint Computer Conference, 29, (1966) p 651.

39. M. Hamilton and Zeldin, "High Order Software - A Methodology for Defining Software," IEEE Trans. Software Eng. SE-2, No. 1 (Mar 1976).

40. Robert L. Hancock, "Microprocessors - Opening Pandora's Box of Computers," Presented at a Conference on Software by American Institute of Industrial Engineers. Washington, D.C. July 19, 1976.

41. William C. Hetzel (ed.), Program Test Methods, Prentice-Hall, Inc. (1973).

42. SAMSO/XXRS-71-1, "Information Proccessing Data Automation Implication of Air Force Command and Control Requirements in the 1980's (CCIP-85): Highlights," 1 (April 1972).

43. Harry Katzan, Jr., Systems Design and Documentation - An Introduction to the HIPO Method, Van Nostrand Reinhold Company (1976).

44. S.R. Kimbleton and Schneider, "Computer Communications Networks," ACM Computing Surveys, 7, No. 3 (Sep 1975).

45. U.S. Department of Commerce, National Technical Information Service, PB-245, 213, "The Feasibility of Software Certification," Ralph E. Keirstead, Jun 1975.

46. B.W. Lampson, "A Scheduling Philosophy for Multiprocessing Systems," Communications ACM, No. 5 (May 1968) p 347.

47. Infotech State of the Art Report 24, "Software Organizations in Computer Networks - Network Systems and Software," H.H. Nagel, (1975) pp 581-598.

48. AFAL-TR-72-292, "Aerospace HOL Computer," William C. Nielsen, A.S. Vere and Joseph A. Lauro, Oct 1972.

49. Robert E. Noonan, "Structured Programming and Formal Specification," IEEE Trans. Software Eng. SE-1, No. 4, (Dec 1975).

50. D.L. Parnas, "A Technique for Software Module Specification with Examples," Com. of the ACM, 15, No. 5 (May 1972) pp 330-335.

51. J.E. Peterson, "Data State Design," Proc. 13th IEEE Computer Soc. Int. Conf. IBM (Sep 7-10, 1976) pp 102-104.

52. Theodore D. Puckorius, "Software Quality in Government," Presented at a Conference on Software, by American Institute of Industrial Engineers, Washington, D.C., (Jul 19, 1976).

53. Raymond J. Rubey, "What's Different About Tactical Military Languages and Compilers," AFIPS Conf. Proc., 42 (1973) pp 807-809.

54. Ronald R. Smith, RADC Structure Programming Series, "Estimating Software Project Resource Requirements," (Jul 1975).

55. Ronald R. Smith, IBM Corporation, Report No. RADC-TR-74-300, "Validation and Verification Study, ' XV, (May 1975).

56. R.T. Yeh (ed.), "A Formal Method for the Design of Operating System Software," Current Trends in Programming Methodology, 1, Prentice Hall, (to be published).

57. University of Michigan, Department of Industrial Engineering, Prospectus and Phase I Report, ISDOS Working Paper No. 1, "ISDOS - A Research Project to Develop Methodology for the Automatic Design and Construction of Information Processing Systems," D. Teichroew and E.H. Sibley, (Oct 1969).

58. T.A. Thayer, "Understanding Software through Emperical Reliability Analysis," AFIPS Conf. Proc., 44 (1975) pp 335.

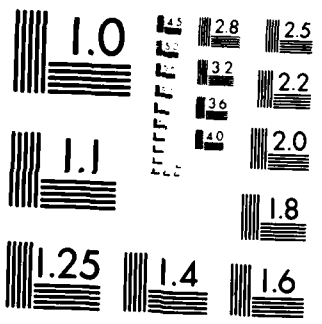
59. Frank Tsui and Lew Priven, "Implementation of Quality Control in Software Development," NCC, 45, 1976.

60. Anthony I. Wasserman, "Issues in Programming Language Design - An Overview," AFIPS Conf. Proc. 44 (1975).

61. Irene M. Watson, "Comparison of Commercially Available Software Tools for Microprocessor Programming," Proc. IEEE, 64, No. 6 (Jun 1976).

AD-A134 583 SYSTEM INTEGRATION AND INTERFACE TRANSITION ISSUES(U) 3/3
DEFENSE COMMUNICATIONS ENGINEERING CENTER RESTON VA
APR 77 DCEC-TR-2-77

UNCLASSIFIED F/G 17/2 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

62. L.G. Stucki, "Guest Editorial," IEEE Trans. Software Eng. SE-2, No. 3 (Sep 1976).

63. Xerox Research Center, Palo Alto, CA., "Report on the Programming Language Euclid," B.W. Lampson, J.J. Horning, R.L. London, J.G. Mitchell and G.J. Popek, Jun 1976.

64. TN 17-75 "The Use of a Communications Oriented Language within a Software Engineering System," P. Cohen, Apr 1975.

DISTRIBUTION LIST (CON'T)

SPECIAL:

Deputy Chief of Staff, Operations and Plans
ATTN: Telecommunications and Command and
Control Directorate (DAMO-TCZ)
Department of the Army
Washington, D.C. 20310

Director, Navy Communications Division
ATTN: NOP 941, Department of the Navy
Washington, D.C. 20310

Director of Command Control and Communications
Headquarters, U.S. Air Force, ATTN: AF/PRC
Washington, D.C. 20330

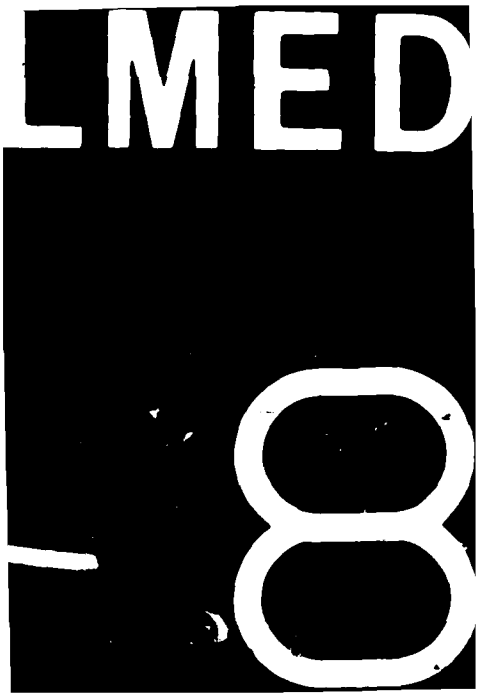
Director, Joint Tactical Communications Office
ATTN: O&M Directorate
Ft. Monmouth, New Jersey 07703

Assistant Director for Communications Security,
National Security Agency, ATTN: S04
Ft. Meade, Maryland 20755

Commander, Naval Telecommunications Command
4410 Massachusettes Avenue, N.W.
Washington, D.C. 20390

Commander, U.S. Army Communications
Command, ATTN: SCC-OPS-PP
Ft. Huachuca, Arizona 85613

Headquarters, Air Force Communications Service
ATTN: XPX, Richards-Gebaur AFB, Missouri 64030


LMED
8